Cybersecurity Technologies, Standards and Operations

Dr David E. Probert

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
1
2
3
4
5

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 • Authentium • BITEK International Inc. • BT Counterpane • Cisco • Cybex • eWorldwide Group • [illegible] • Intel Corporation • Microsoft Corporation • [illegible] • [illegible] • UMTS Forum • VeriSign • Asia Pacific Economic Cooperation Telecommunications and Information Working Group (APECTel) • African Telecommunications Union (ATU) • Commonwealth Telecommunications Organization (CTO) • Computer Emergency Response Team (CERT) • 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).

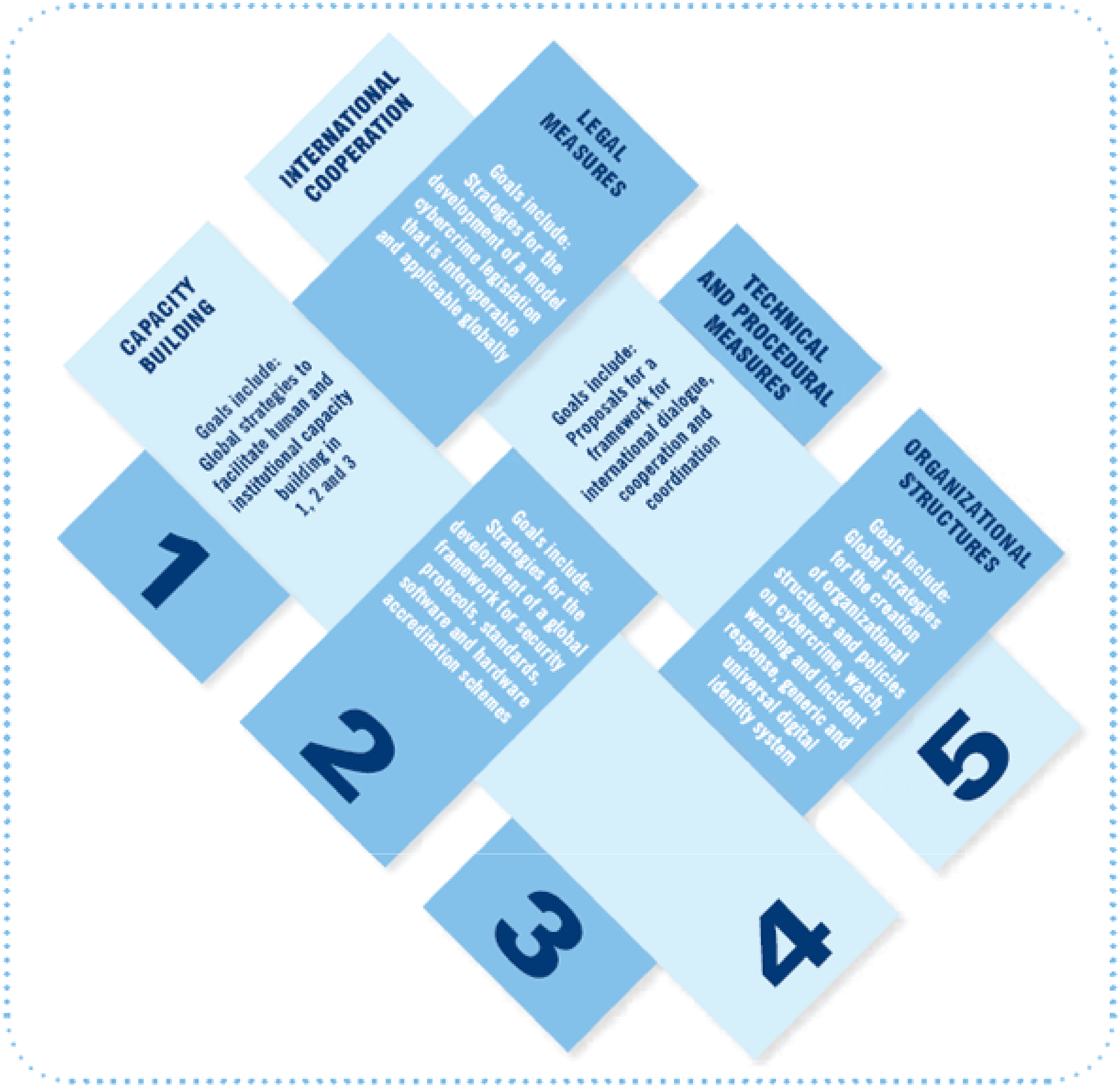
The experts have been invited to join the HLEG because of their world-renowned expertise in the [illegible] areas of the GCA and they participate in a personal capacity.

[1] [illegible]

ITU: Committed to connecting the world

International Telecommunication Union

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

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

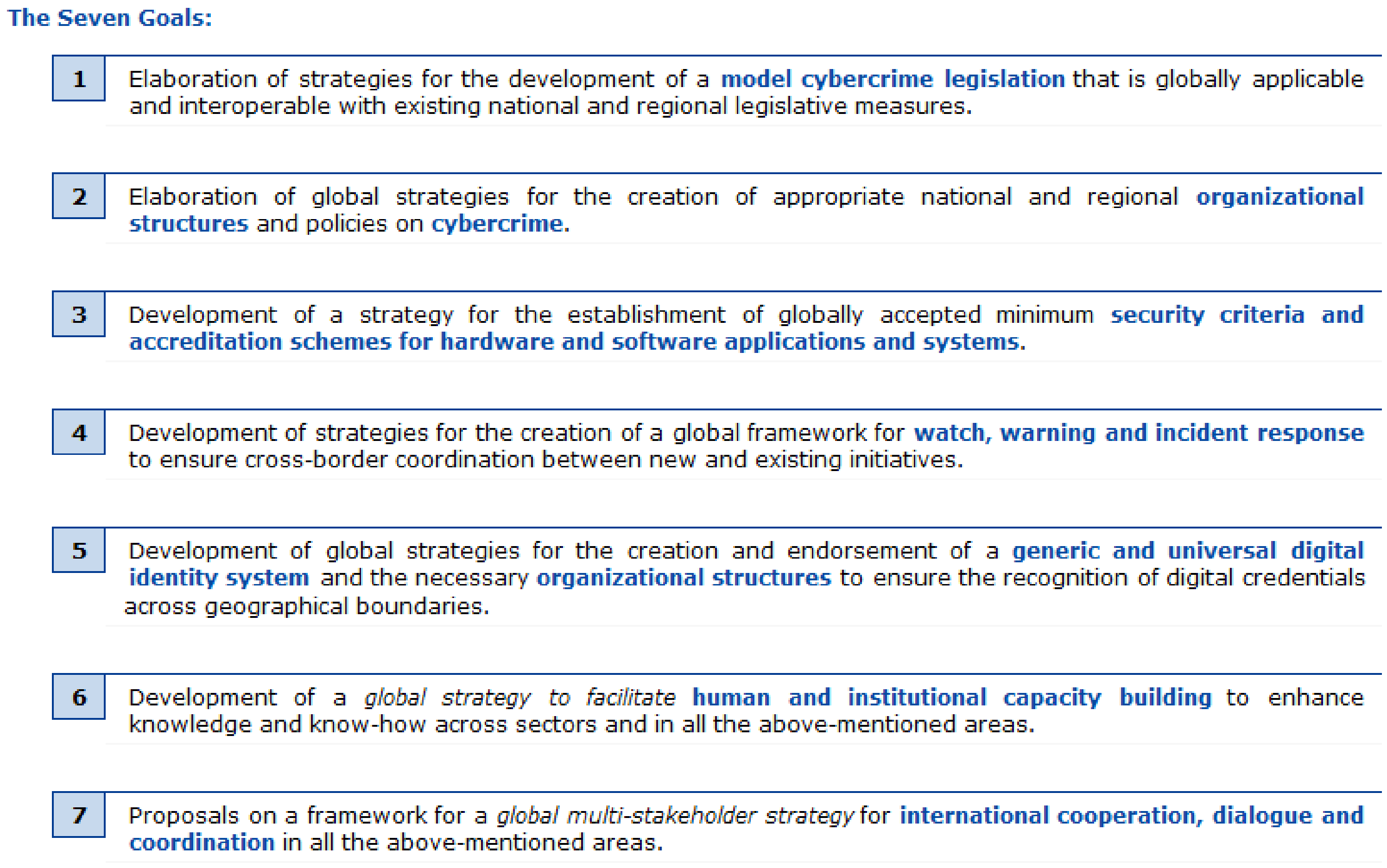
ORGANIZATIONAL STRUCTURES

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

The ITU GCA - Global Cybersecurity Agenda:

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

ITU GCA – Seven Strategic Goals



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.**

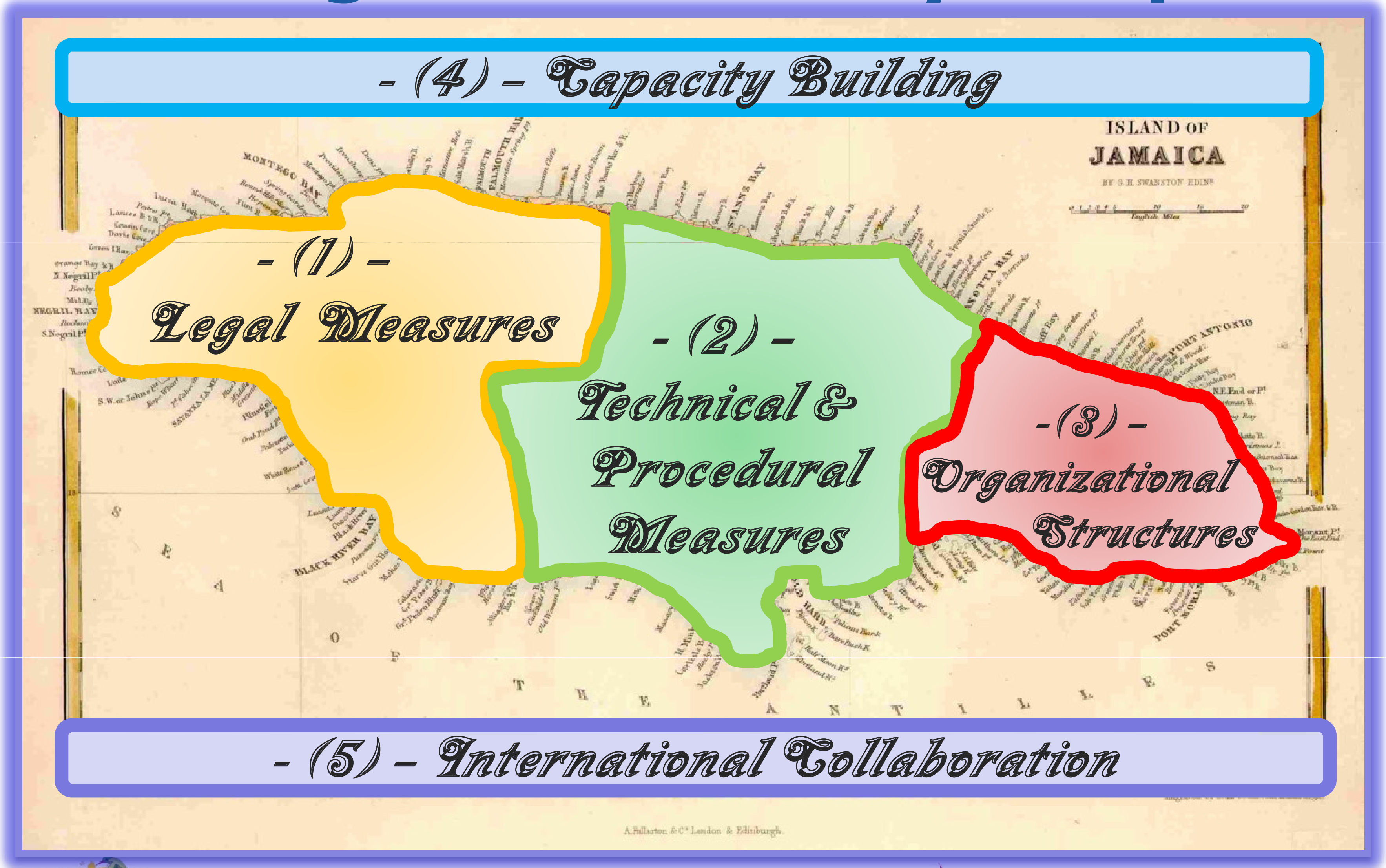
4 Development of strategies for the creation of a global framework for **watch, warning and incident response** to ensure cross-border coordination between new and existing initiatives.

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.

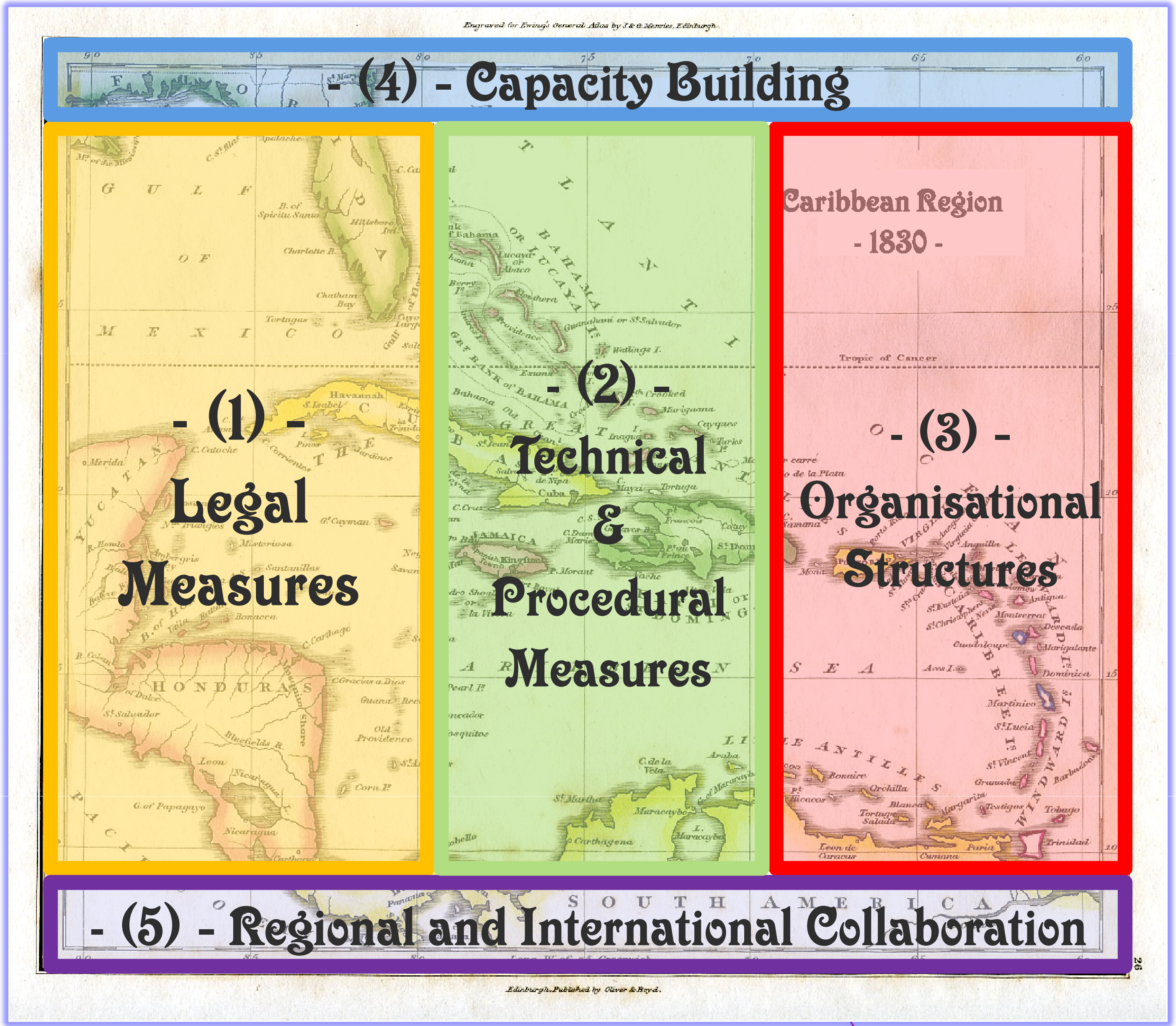
6 Development of a *global strategy to facilitate* **human and institutional capacity building** to enhance knowledge and know-how across sectors and in all the above-mentioned areas.

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

Securing Jamaica in Cyberspace!



Securing the Caribbean in Cyberspace!


Engraved for Ewing's General Atlas by J & G. Menzies, Edinburgh.
- (4) - Capacity Building
- (1) - Legal Measures
- (2) - Technical & Procedural Measures
- (3) - Organisational Structures
Caribbean Region
- 1830 -
- (5) - Regional and International Collaboration
Edinburgh. Published by Oliver & Boyd.

University of Technology, Jamaica

ITU Centres of Excellence Network for the Caribbean Region
Cybersecurity Technologies, Standards & Operations
16-17 September, Kingston, Jamaica

International Telecommunication Union
Committed to connecting the world

* ITU Workshop Overview*

"Cybersecurity Technologies, Standards & Operations"

Workshop Presentations | *Group Tasks & Discussions*

S1-Thurs: 9:30-11:00 "The International Cybercrime and Cybersecurity Challenge"	S2–Thurs:11:30-13:00 "Integration Cyber-Technological Solutions for the 21stC Web2.0 World"	S3-Thurs:14:00-15:30 Group Session: "Securing Critical Computing and Network Facilities"	S4-Thurs:16:00-17:30 Group Session: "Group Discussion: Securing Critical Computing and Network Facilities"
S5 - Fri: 9:30–11:00 "Cybersecurity Continuity Planning, Standards and Architectures"	S6 – Fri: 11:30–13:00 "Organising a National Crime Unit and CERT/CSIRT"	S7 – Fri: 14:00-15:30 Group Session: "Designing Practical Cybercrime Solutions – Critical Sectors"	S7 – Fri: 16:00-17:30 Group Session" "Group Discussion: Designing Practical Cybercrime Solutions – Critical Sectors"

* ITU Workshop Overview*

“Cybersecurity Technologies, Standards & Operations”

S1-Thurs: 9:30-11:00 “The International Cybercrime and Cybersecurity Challenge”	S2–Thurs:11:30-13:00 “Integration Cyber-Technological Solutions for the 21stC Web2.0 World”	S3-Thurs:14:00-15:30 Group Session: “Securing Critical Computing and Network Facilities”	S4-Thurs:16:00-17:30 Group Session: “Group Discussion: Securing Critical Computing and Network Facilities”
S5 - Fri: 9:30–11:00 “Cybersecurity Continuity Planning, Standards and Architectures”	S6 – Fri: 11:30–13:00 “Organising a National Crime Unit and CERT/CSIRT”	S7 – Fri: 14:00-15:30 Group Session: “Designing Practical Cybercrime Solutions – Critical Sectors”	S7 – Fri: 16:00-17:30 Group Session” “Group Discussion: Designing Practical Cybercrime Solutions – Critical Sectors”

* Workshop Session 1 *

“The International Cybercrime and Cybersecurity Challenge”

1 –Aim: National Cybersecurity	2 – Review Strategy & Plans	3 – Cyber Threats & Crimes
4 – Cyber Technical Threats	5 – Operational Security	6 – Critical Economic Sectors
7 – Case Study: Governments	8 – Case Study: Banks/Finance	9 – Key Jamaican Sectors

* Workshop Session 1 *

“The International Cybercrime and Cybersecurity Challenge”

1 –Aim: National Cybersecurity	2 – Review Strategy & Plans	3 – Cyber Threats & Crimes
4 – Cyber Technical Threats	5 – Operational Security	6 – Critical Economic Sectors
7 – Case Study: Governments	8 – Case Study: Banks/Finance	9 – Key Jamaican Sectors

Aim: Jamaican & Caribbean Cybersecurity

- *Aim:* To focus on the ITU Global Cybersecurity Agenda's "Technical & Operational Measures" which will help secure the Caribbean in Cyberspace

- *Agenda:* During the 2-Day Workshop we'll review the cyber threats, technical standards, architectures, & specific organisational models

- *Focus:* A full in-depth technical course on cybersecurity such as those run by ITU/IMPACT would take 8 to 12 weeks to cover the complete spectrum of topics required for professional certification such as CISSP.

- *Essentials*: Hence during these 2 days we'll work together on the technical essentials that will serve as a strong foundation to your future studies & practical implementations of cybersecurity solutions & operations

* Workshop Session 1 *

“The International Cybercrime and Cybersecurity Challenge”

1 –Aim: National Cybersecurity	2 – Review Strategy & Plans	3 – Cyber Threats & Crimes
4 – Cyber Technical Threats	5 – Operational Security	6 – Critical Economic Sectors
7 – Case Study: Governments	8 – Case Study: Banks/Finance	9 – Key Jamaican Sectors

Review Strategy & Cyber Plans

- The ITU Cybersecurity Agenda spans 5 Operational Pillars and 7 Strategic Goals. These were presented and comprehensively discussed during the preceeding 3-day ITU Cybersecurity Workshop at UTECH

- The technical & operational measures against cyberattacks, cyberterrorism and cybercrime are only effective when embedded within a total national & enterprise driven management plan including:
  - National Strategy: Jamaica Government and leading enterprises will need to define and communicate its top-level strategic cybersecurity objectives
  - Cybersecurity Agency: Many countries have created a dedicated National Cybersecurity Agency that is designated with the authority, budget & responsibility for the co-ordination of all aspects of the cybersecurity agenda across government, institutions & business
  - Action Plans & RoadMap: During 13th to 15th Sept we worked together as a group on the develop of outline action plans and roadmaps for both the Jamaican Government as well as enterprises and institutions that comprise Jamaica's critical service sectors

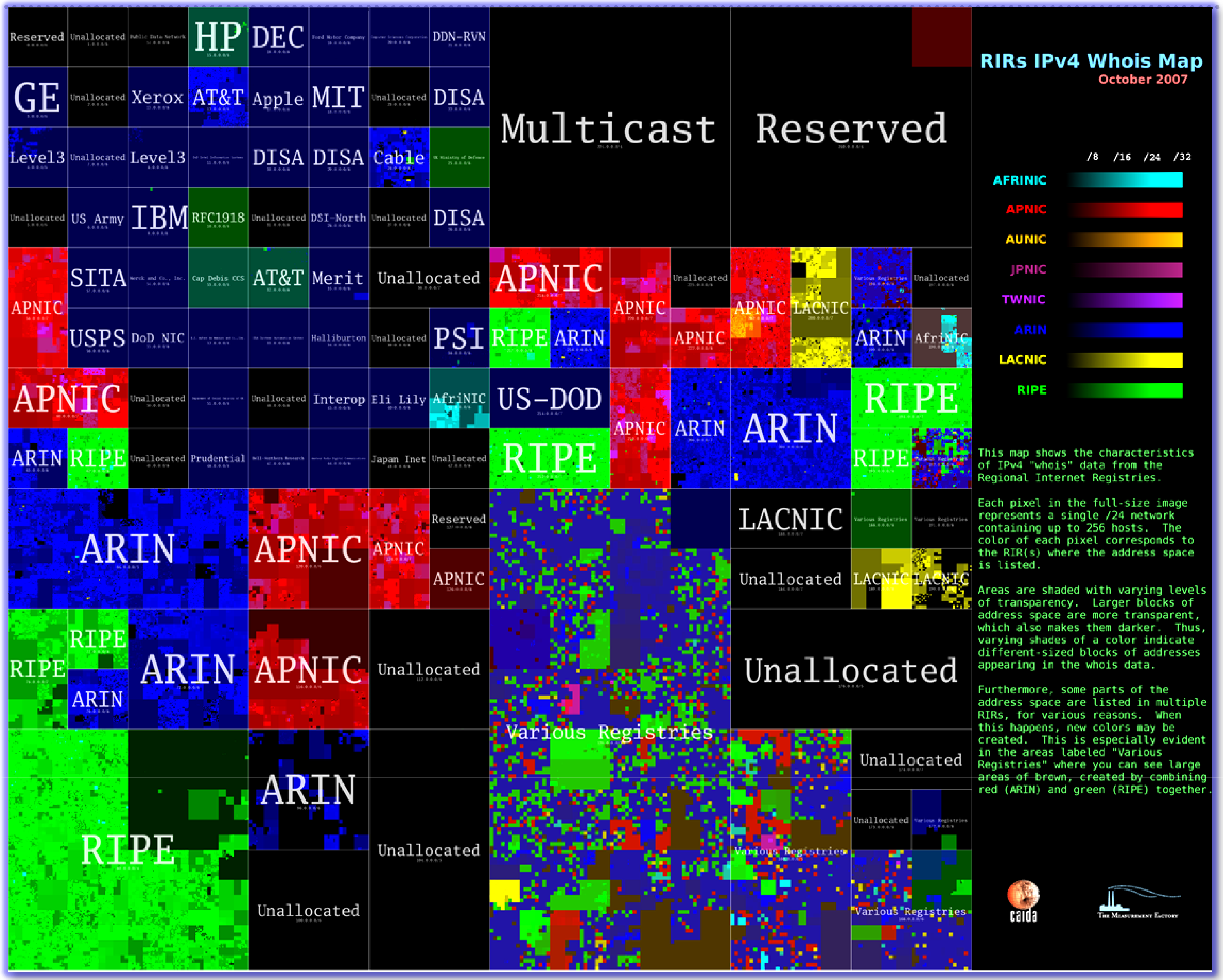
- Next we shall proceed with our focus on technical threats & solutions…

* Workshop Session 1 *

“The International Cybercrime and Cybersecurity Challenge”

1 –Aim: National Cybersecurity	2 – Review Strategy & Plans	3 – Cyber Threats & Crimes
4 – Cyber Technical Threats	5 – Operational Security	6 – Critical Economic Sectors
7 – Case Study: Governments	8 – Case Study: Banks/Finance	9 – Key Jamaican Sectors

"Visualisation of Cyberspace": Global IP WHOIS Addresses



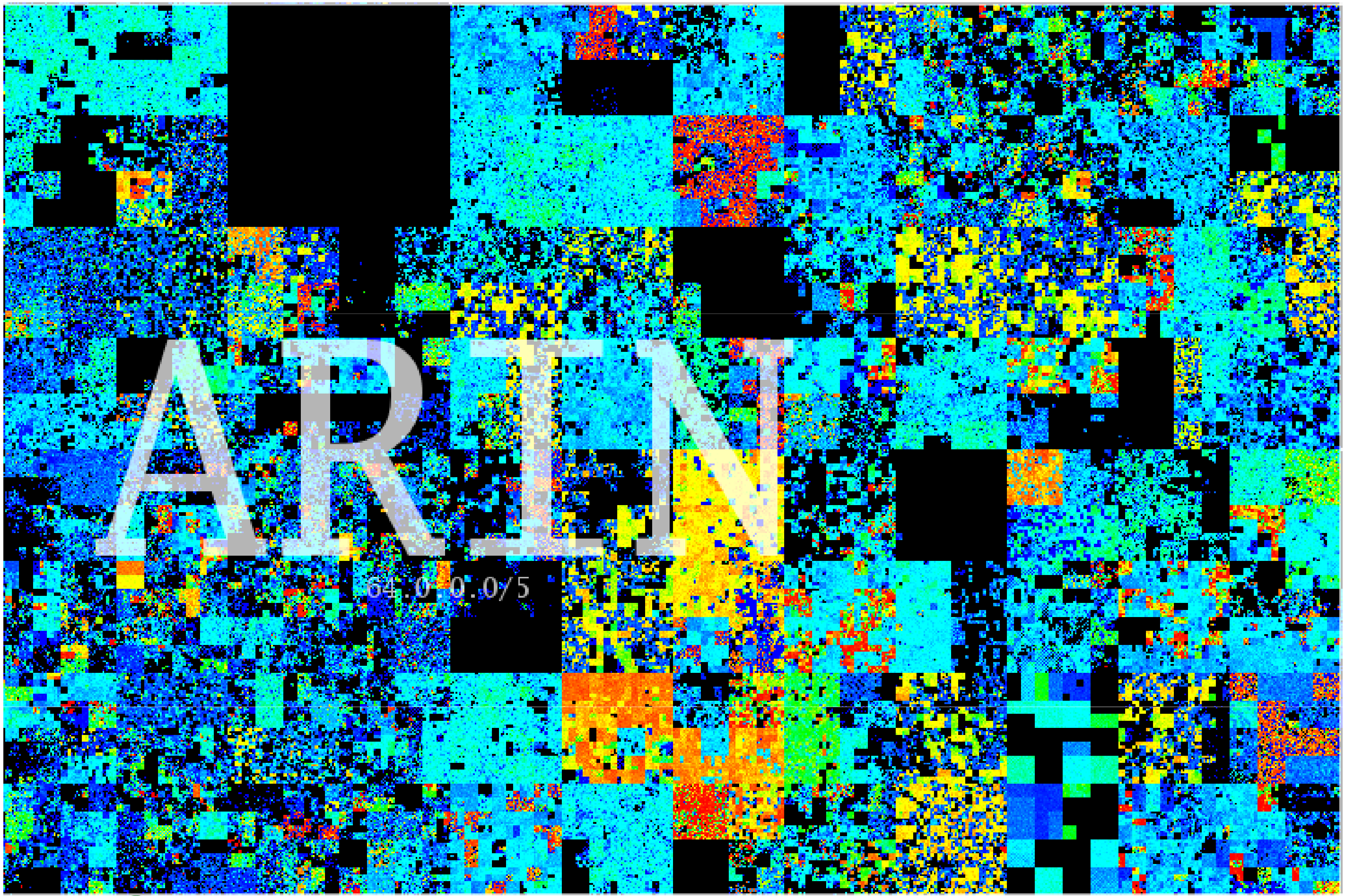
This map shows the characteristics of IPv4 "whois" data from the Regional Internet Registries.

Each pixel in the full-size image represents a single /24 network containing up to 256 hosts. The color of each pixel corresponds to the RIR(s) where the address space is listed.

Areas are shaded with varying levels of transparency. Larger blocks of address space are more transparent, which also makes them darker. Thus, varying shades of a color indicate different-sized blocks of addresses appearing in the whois data.

Furthermore, some parts of the address space are listed in multiple RIRs, for various reasons. When this happens, new colors may be created. This is especially evident in the areas labeled "Various Registries" where you can see large areas of brown, created by combining red (ARIN) and green (RIPE) together.

Active Internet Domains – "American IP Registry"

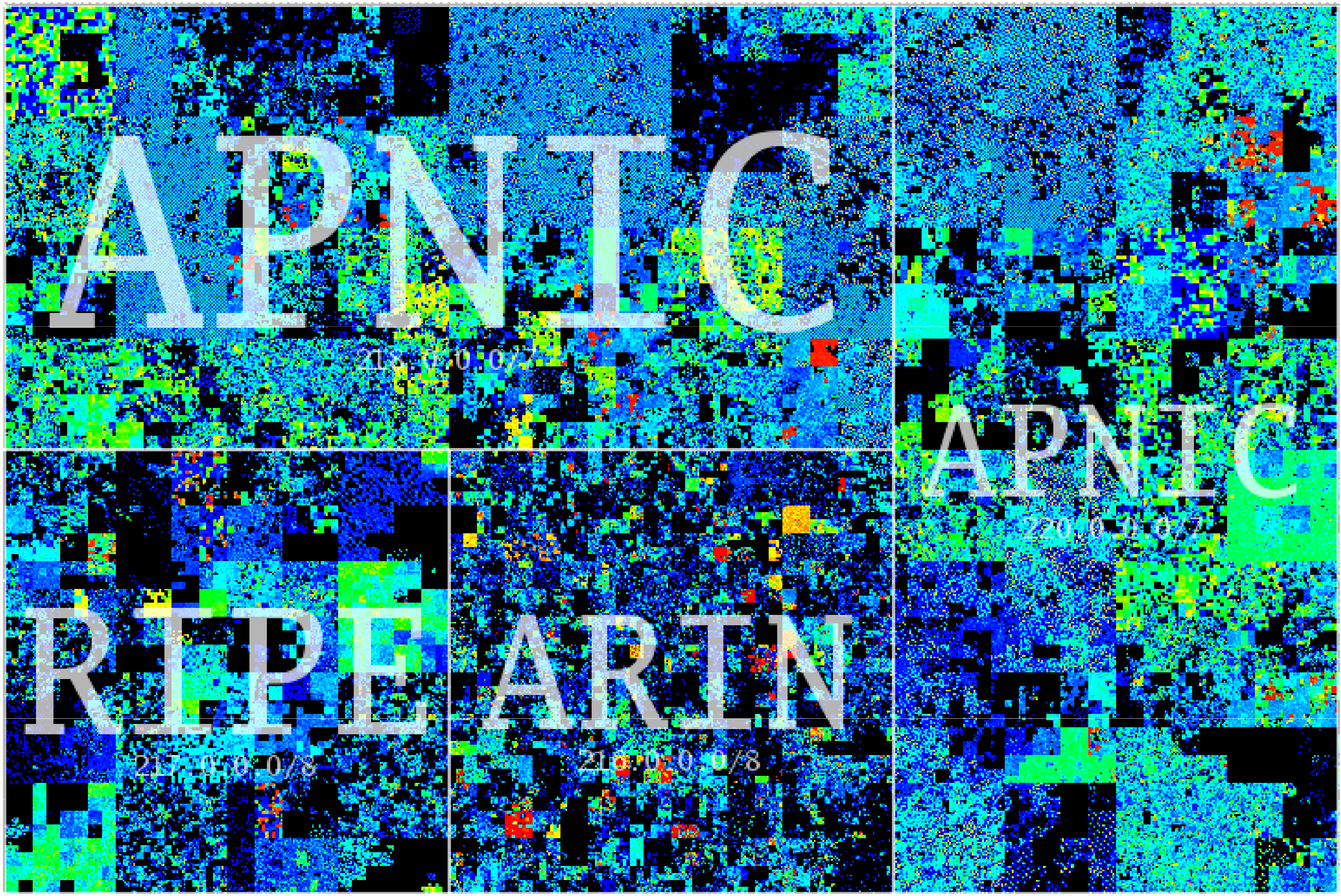


University of Technology, Jamaica

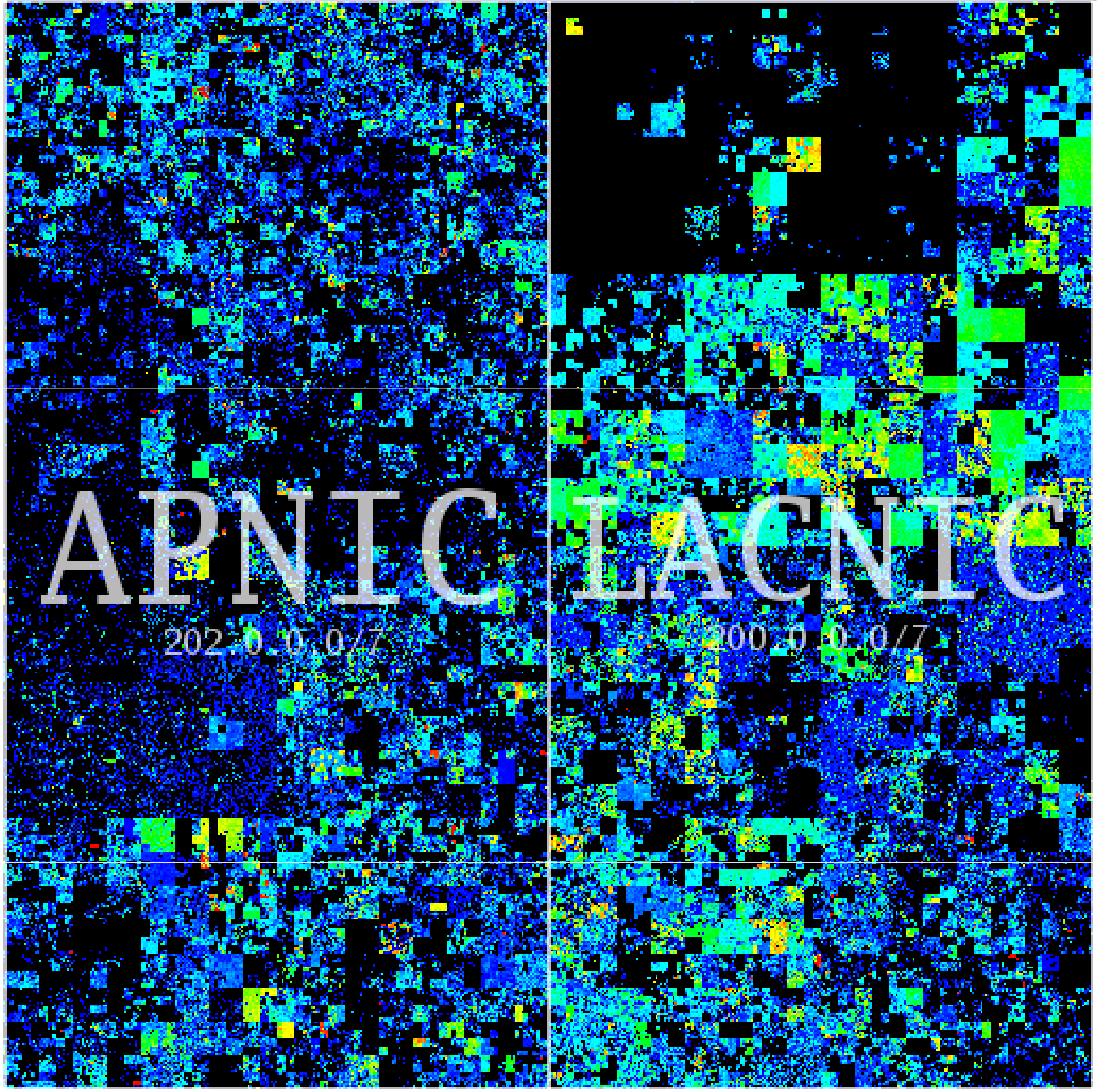
ITU Centres of Excellence Network for the Caribbean Region
Cybersecurity Technologies, Standards & Operations
16-17 September, Kingston, Jamaica

International Telecommunication Union
Committed to connecting the world

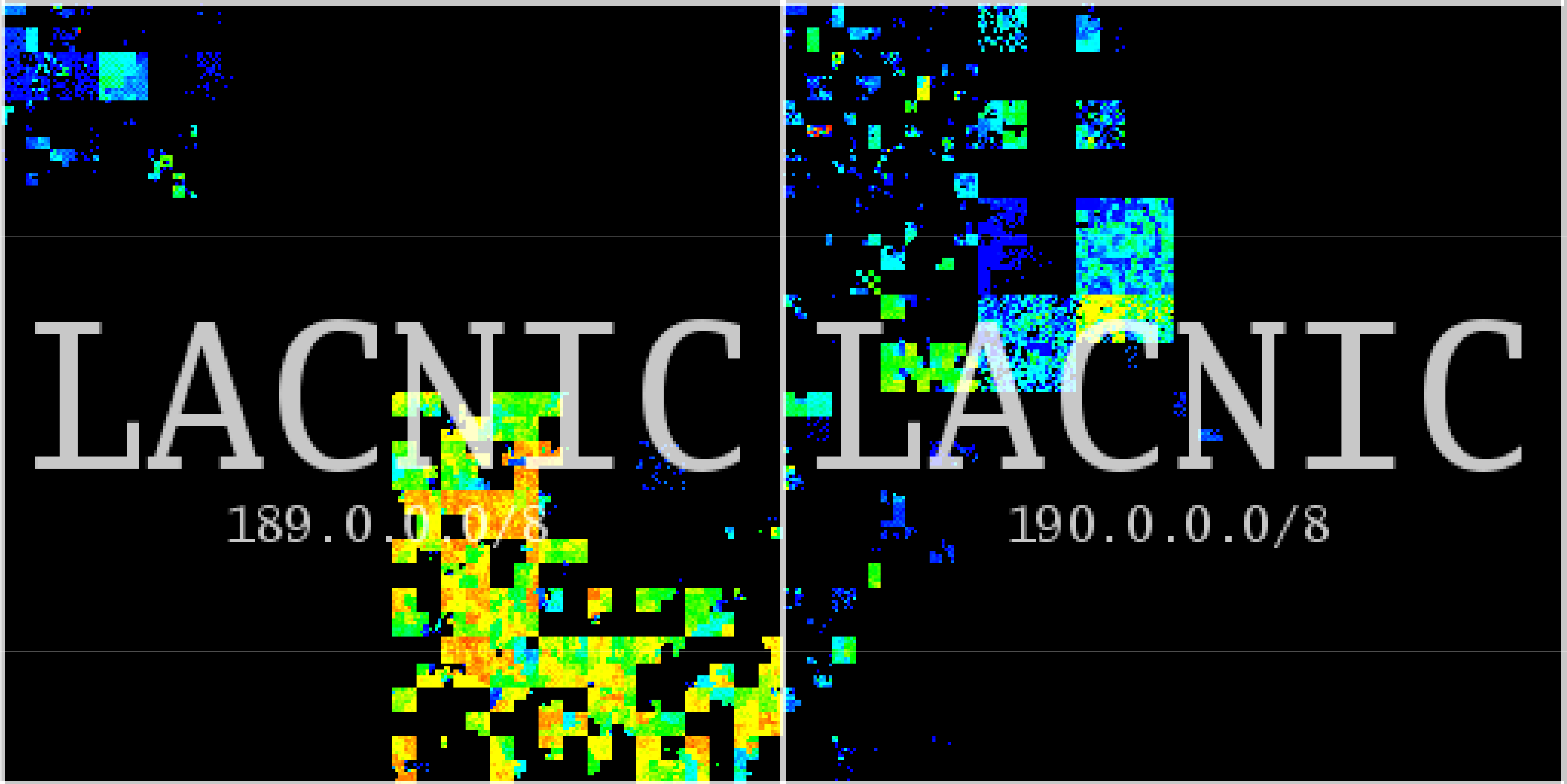
Visual IP Cyberspace: Asia-Pacific, Europe & America



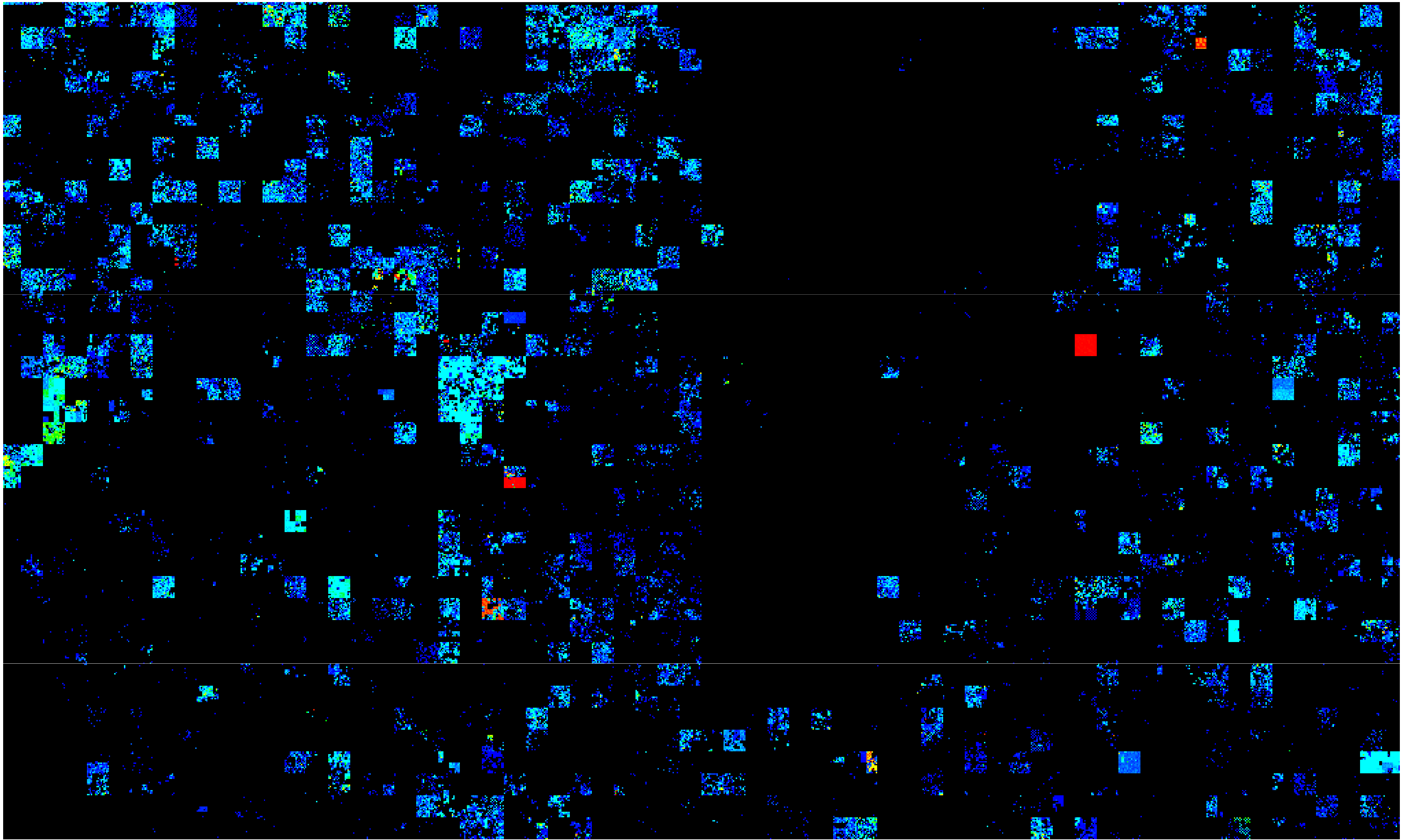
IP Cyberspace: Asia-Pacific, Latin America and Caribbean



Latin America and Caribbean: “LACNIC”



“Outer Galaxies of Cyberspace” – Other Registries

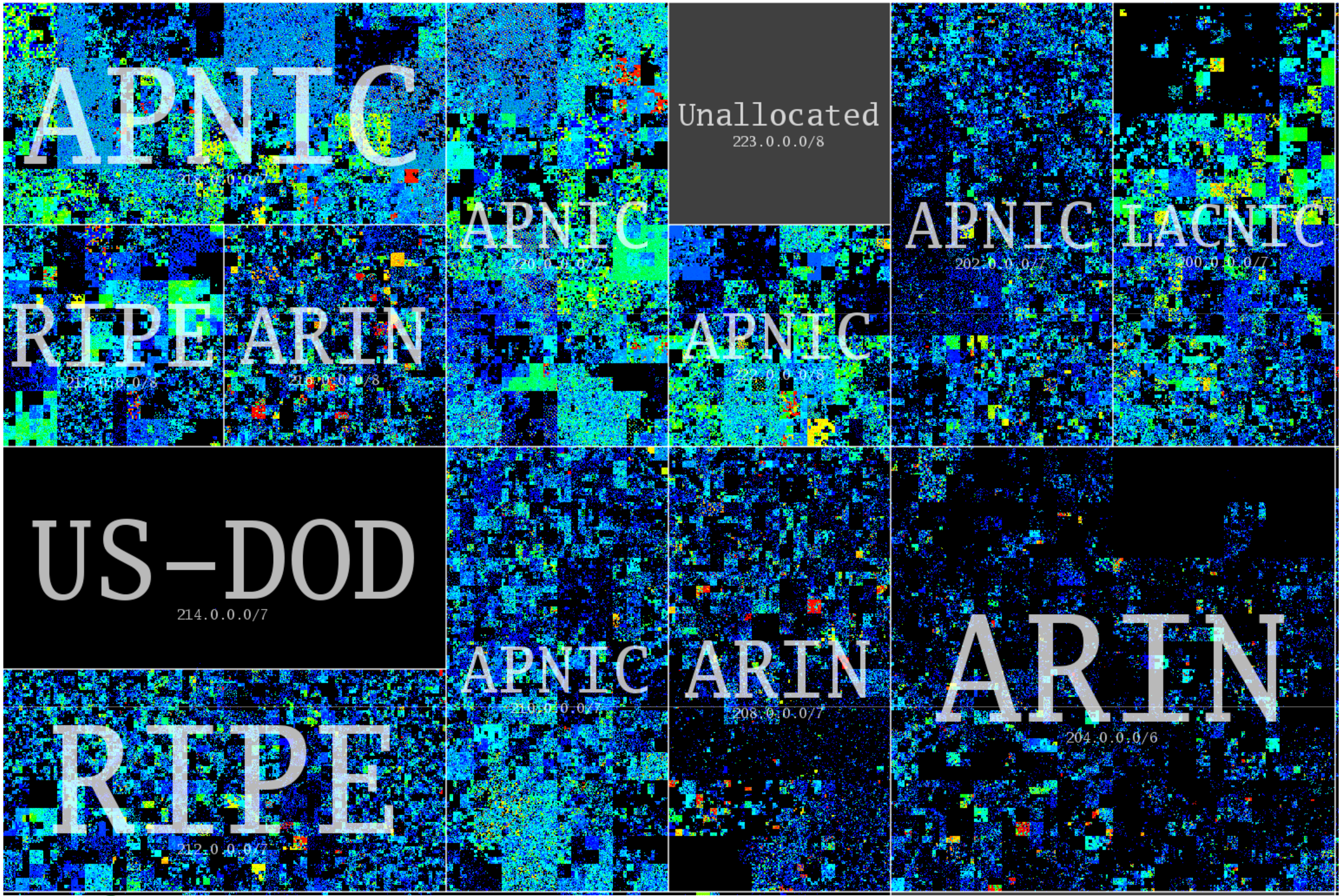


University of Technology, Jamaica

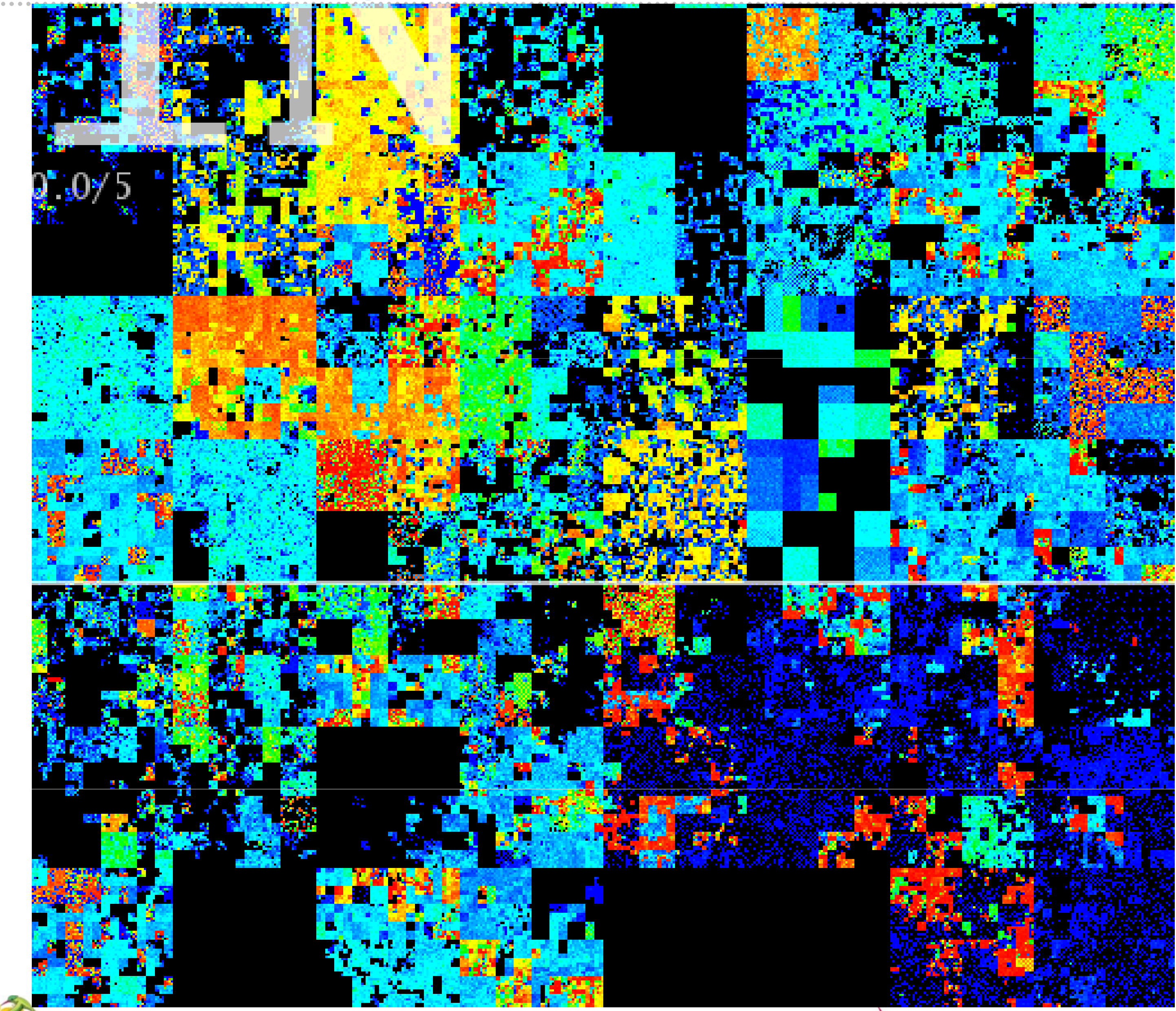
ITU Centres of Excellence Network for the Caribbean Region
Cybersecurity Technologies, Standards & Operations
16-17 September, Kingston, Jamaica

International Telecommunication Union
Committed to connecting the world

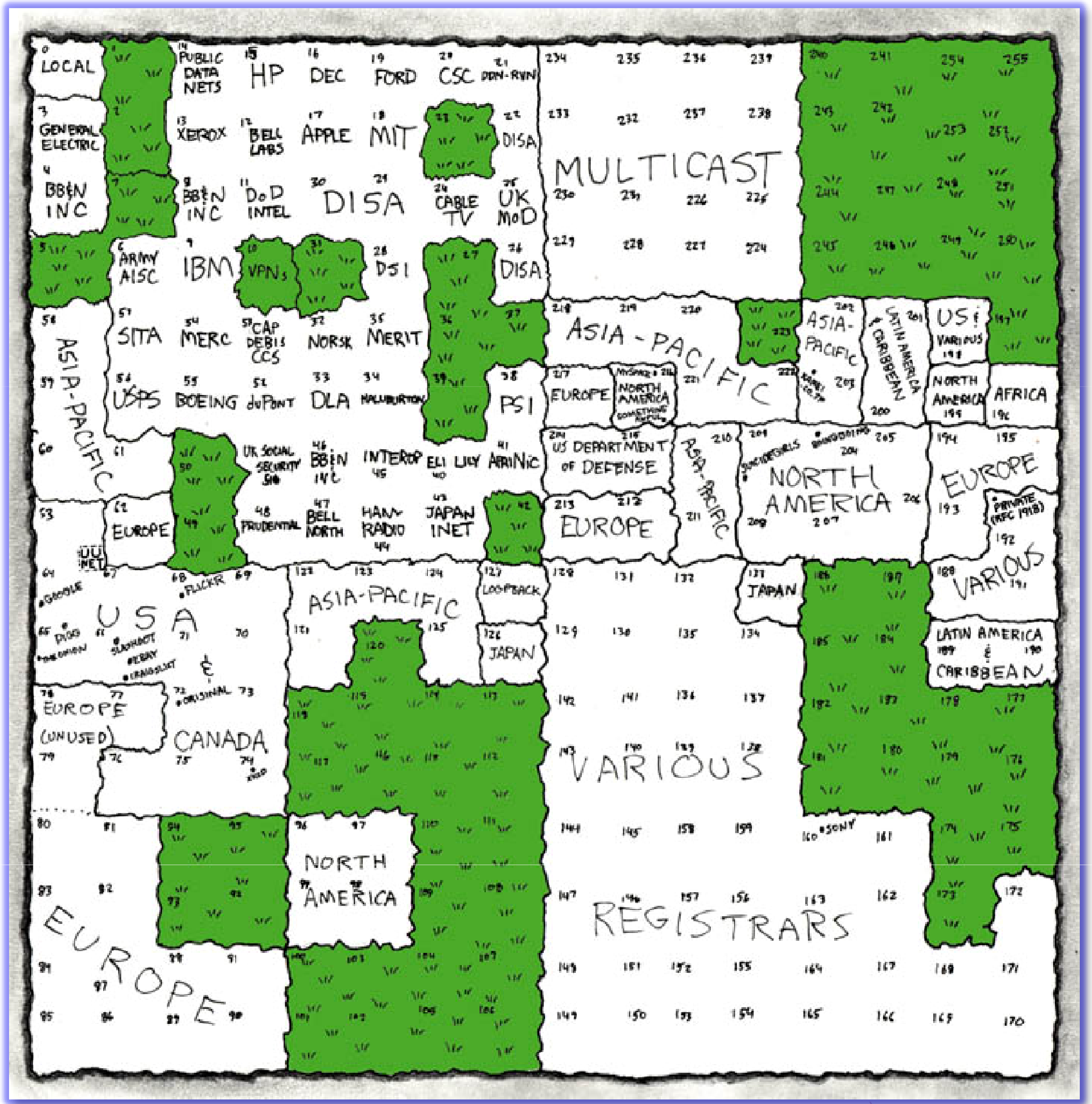
Densely Populated Regions of IP Cyberspace



The Challenging Complexity of IP Cyberspace



Cyberspace *"Hilbert Map"* of Global IP Addresses



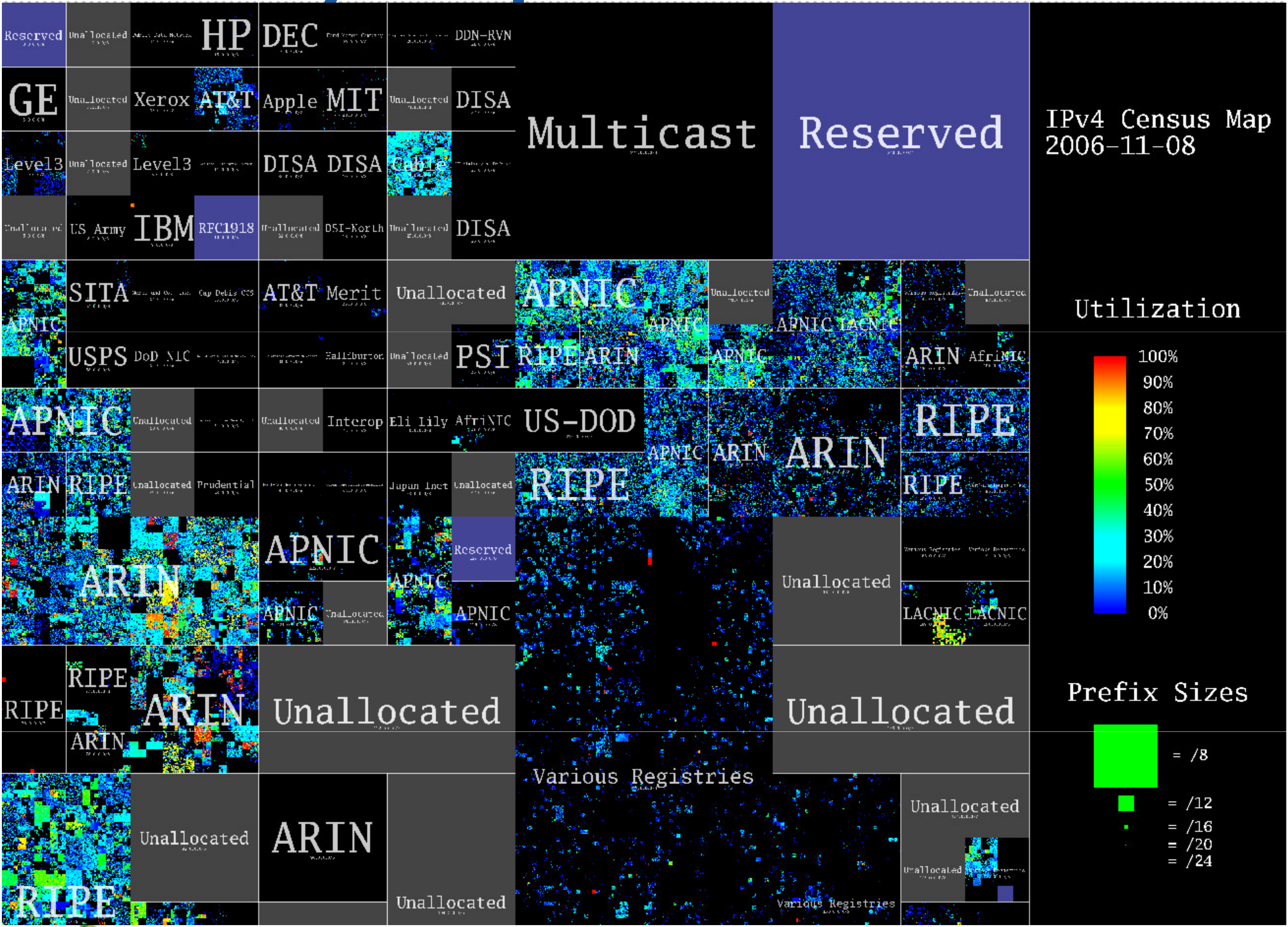
ITU Centres of Excellence Network for the Caribbean Region
Cybersecurity Technologies, Standards & Operations
16-17 September, Kingston, Jamaica

University of Technology, Jamaica

International Telecommunication Union

Committed to connecting the world

Global Cyberspace IP Census - 2006

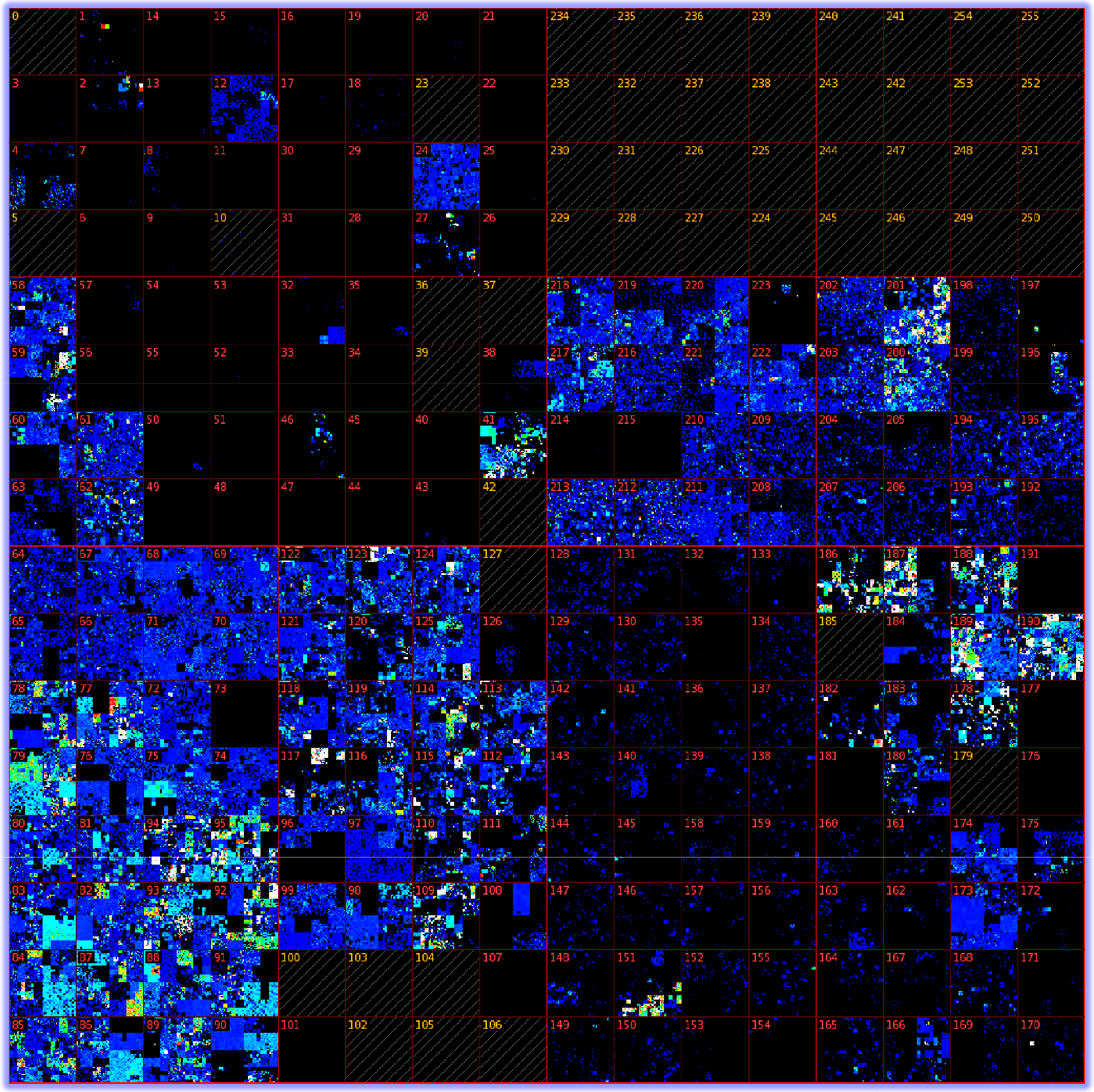


ITU Centres of Excellence Network for the Caribbean Region
Cybersecurity Technologies, Standards & Operations
16-17 September, Kingston, Jamaica

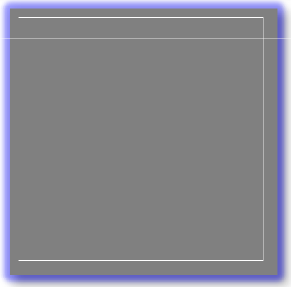
University of Technology, Jamaica

International Telecommunication Union
Committed to connecting the world

Global Malicious Activity in *"Hilbert"* IP Cyberspace



Key: Hilbert Space-Filling Curve Process



Link: www.team-cymru.org

University of Technology, Jamaica

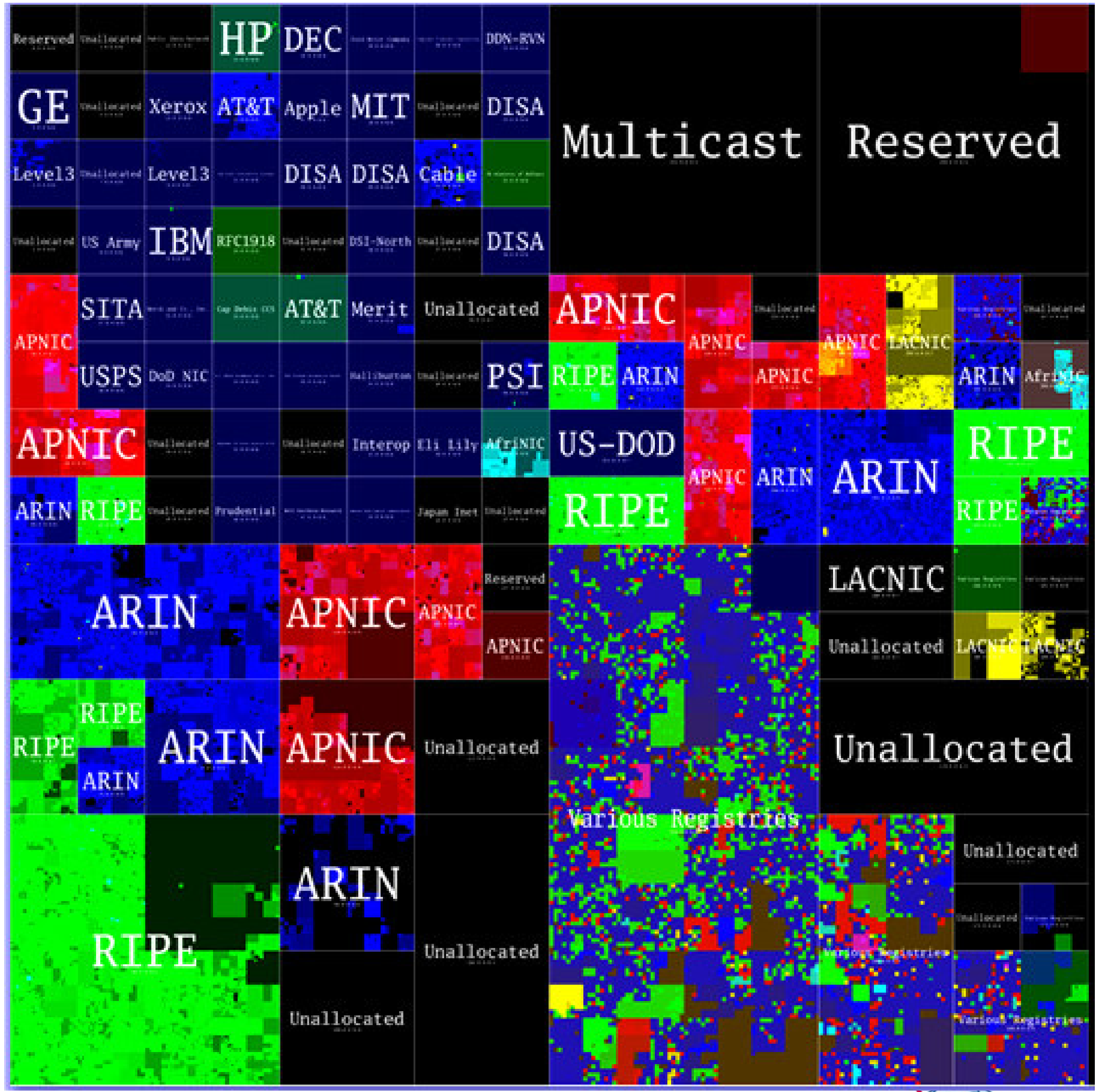
ITU Centres of Excellence Network for the Caribbean Region
Cybersecurity Technologies, Standards & Operations
16-17 September, Kingston, Jamaica

International Telecommunication Union

Committed to connecting the world

Basis for Visualisation of Global IP Cyberspace:

- Hilbert Space Filling Fractal Curve Process -

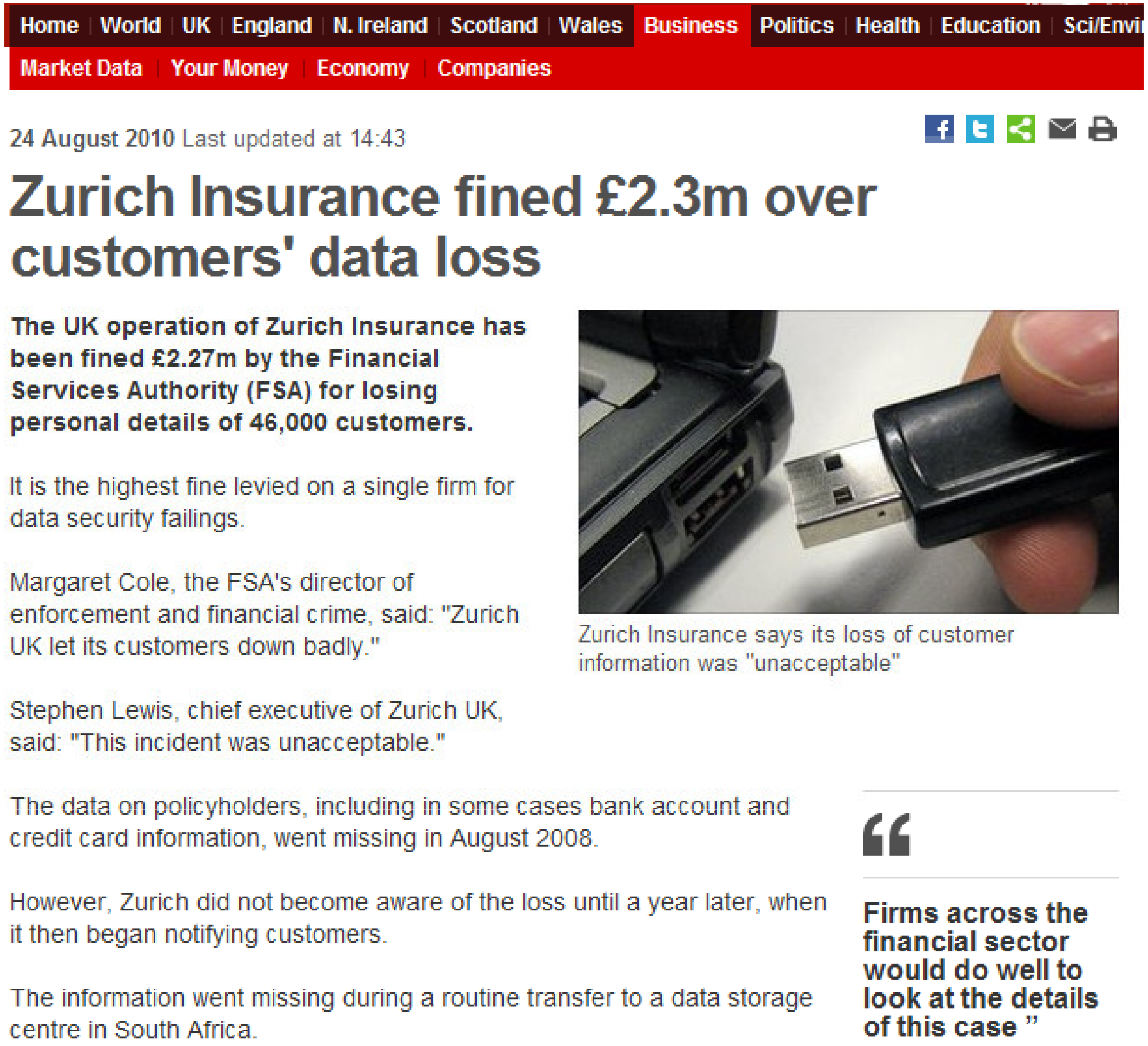


University of Technology, Jamaica

Cyber Threats and Crimes

- Wide Spectrum: Cyberthreats & Cybercrimes span a vast spectrum of malicious and potentially illegal activity in cyberspace with various motivations.
- Modes of Attack: The modes of cyberattack will also vary according to the criminal or terrorist "business plan" and objectives. These modes will be discussed later, and then we'll summarise the technical & operational solutions
- Industrialisation: Cybercrime is now mainstream and the tools and techniques have now been "industrialised" including "botnets" and mailing lists for hire, and stolen credit card and banking details available for "on-line sale"
  - Financial Gain: Criminals hacking into bank accounts, credit cards, stealing personal IDs
  - Targeted Disruption: Terrorists hiring "botnets" to target critical national infrastructure
  - Revenge Attacks: Redundant Staff & Others that steal company information & databases
  - Personal Attacks: On-line attacks using social networking to discredit & smear enemies
  - Political Attacks: Spread of malicious and false political propaganda through viral marketing campaigns orchestrated through social networks

Financial Services: Personal Data Loss



24 August 2010 Last updated at 14:43

Zurich Insurance fined £2.3m over customers' data loss

The UK operation of Zurich Insurance has been fined £2.27m by the Financial Services Authority (FSA) for losing personal details of 46,000 customers.

Zurich Insurance says its loss of customer information was "unacceptable"

It is the highest fine levied on a single firm for data security failings.

Margaret Cole, the FSA's director of enforcement and financial crime, said: "Zurich UK let its customers down badly."

Stephen Lewis, chief executive of Zurich UK, said: "This incident was unacceptable."

The data on policyholders, including in some cases bank account and credit card information, went missing in August 2008.

However, Zurich did not become aware of the loss until a year later, when it then began notifying customers.

The information went missing during a routine transfer to a data storage centre in South Africa.

> **“ Firms across the financial sector would do well to look at the details of this case ”**

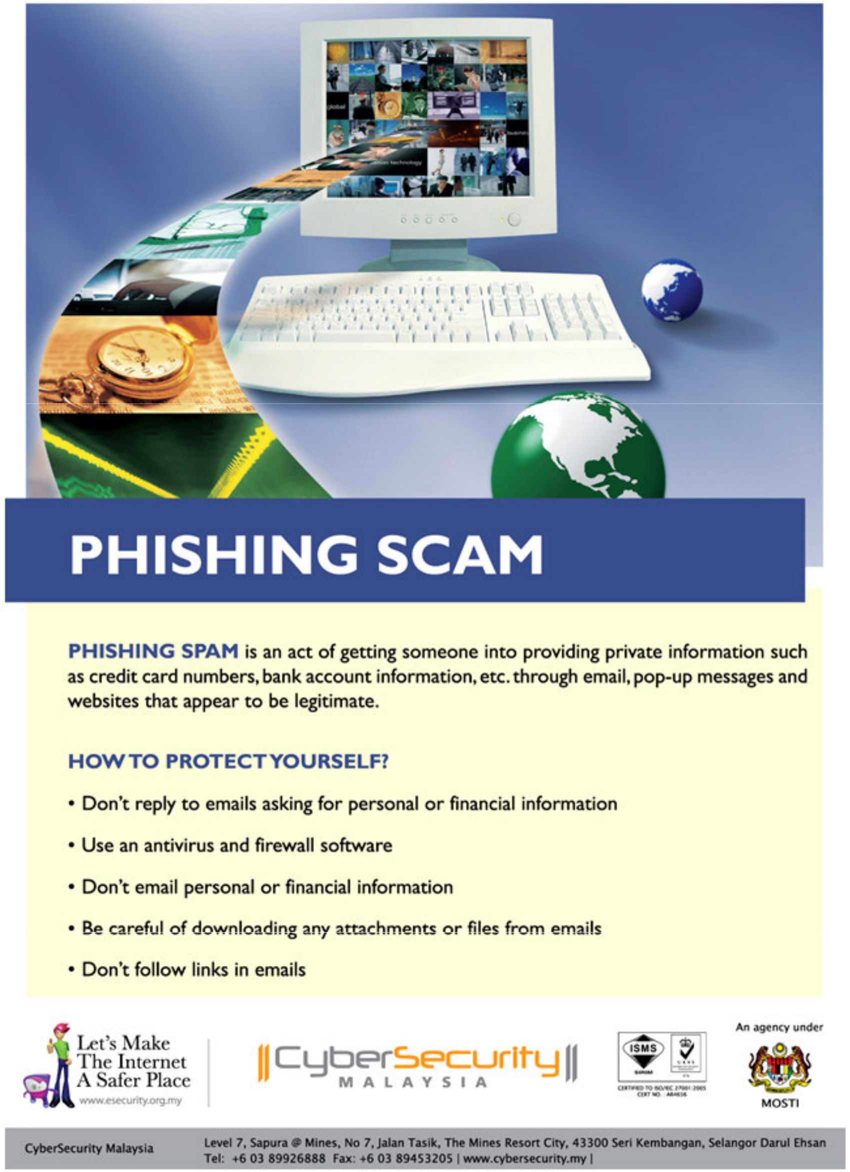
“Cybersecurity Malaysia”

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

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

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

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?

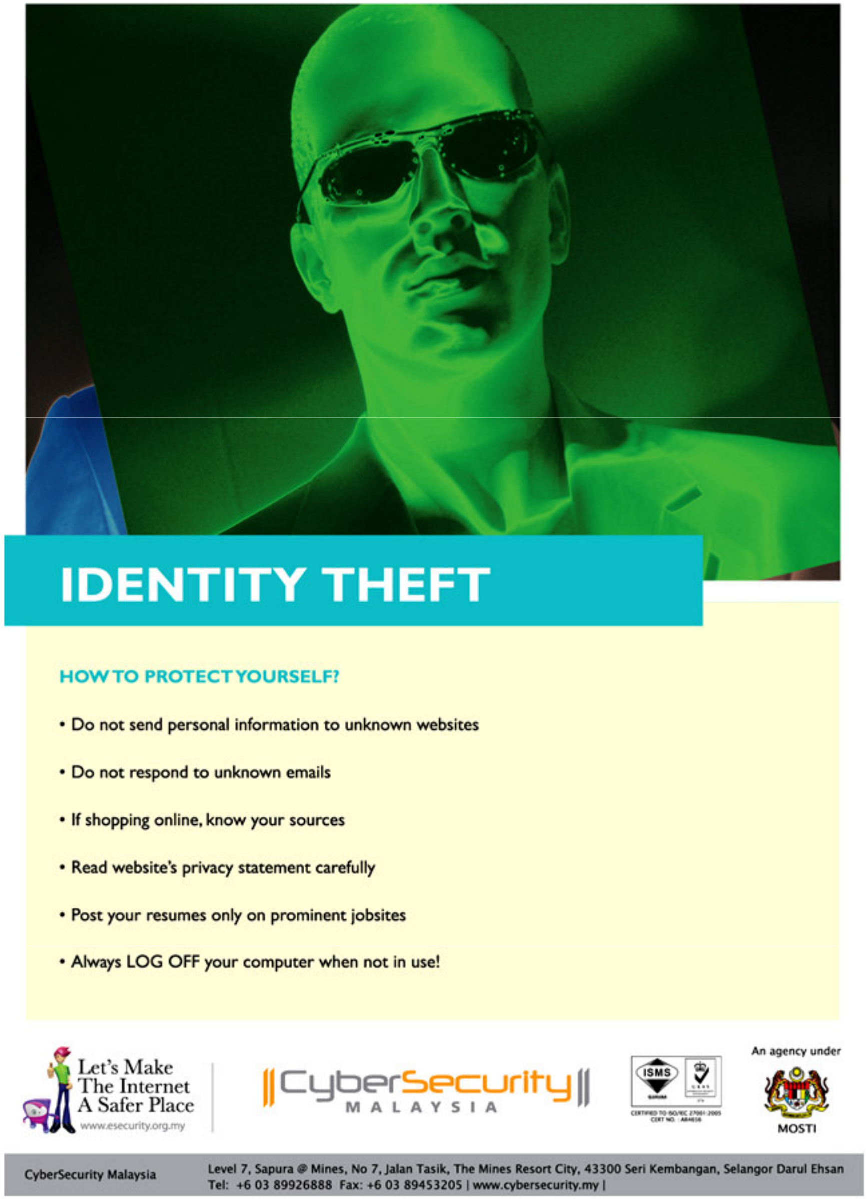
- Don't reply to emails asking for personal or financial information
- Use an antivirus and firewall software
- Don't email personal or financial information
- Be careful of downloading any attachments or files from emails
- Don't follow links in emails

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

CyberSecurity MALAYSIA

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!

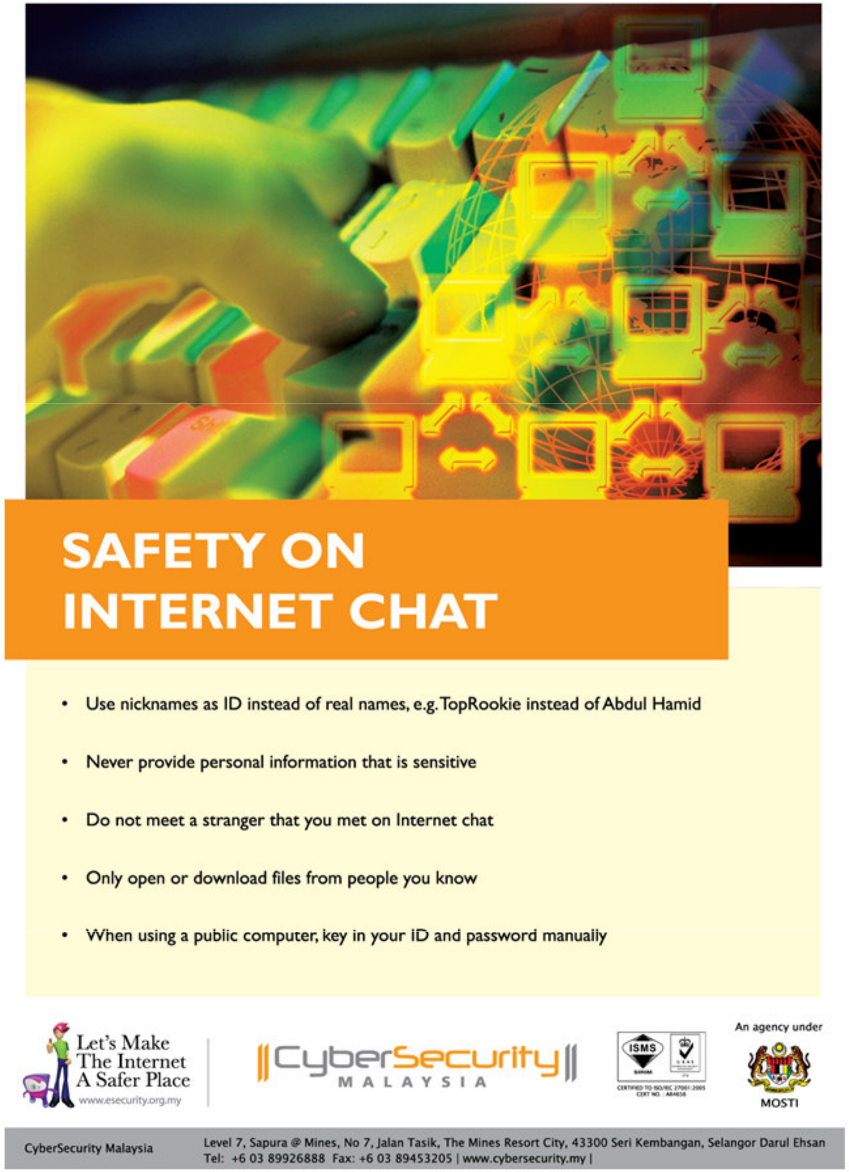
Let's Make The Internet A Safer Place
www.esecurity.org.my

CyberSecurity MALAYSIA

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 |

Internet Chat and Spam eMail



SAFETY ON INTERNET CHAT

- Use nicknames as ID instead of real names, e.g. TopRookie instead of Abdul Hamid
- Never provide personal information that is sensitive
- Do not meet a stranger that you met on Internet chat
- Only open or download files from people you know
- When using a public computer, key in your ID and password manually

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

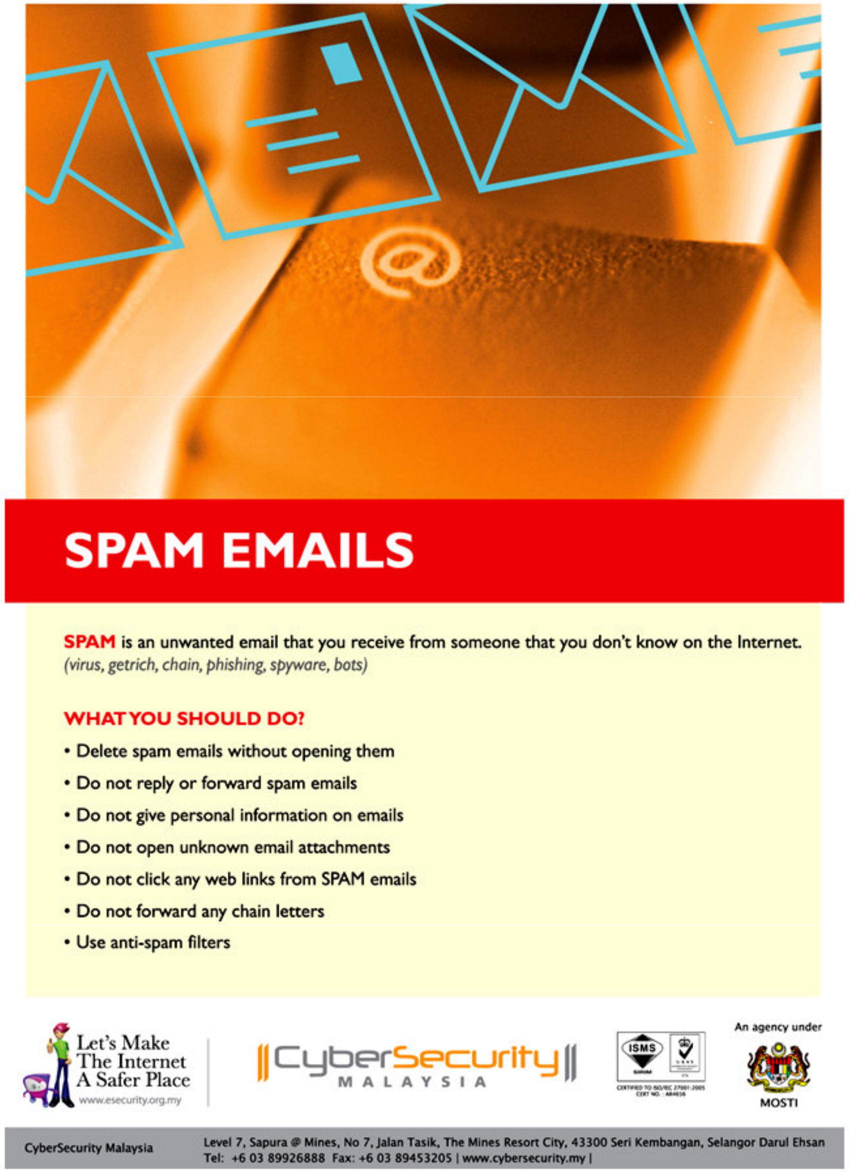
CyberSecurity MALAYSIA

ISMS CERTIFIED TO ISO/IEC 27001:2005 CERT NO. : AR4656

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 |



SPAM EMAILS

SPAM is an unwanted email that you receive from someone that you don't know on the Internet.
(virus, getrich, chain, phishing, spyware, bots)

WHAT YOU SHOULD DO?

- Delete spam emails without opening them
- Do not reply or forward spam emails
- Do not give personal information on emails
- Do not open unknown email attachments
- Do not click any web links from SPAM emails
- Do not forward any chain letters
- Use anti-spam filters

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

CyberSecurity MALAYSIA

ISMS CERTIFIED TO ISO/IEC 27001:2005 CERT NO. : AR4656

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 |

On-Line Shopping and Banking

http://www.
Online Shopping

SHOP SAFELY ONLINE

- Shop with merchants that you know or trust
- Check that the shopping website is secured
- Be wary of unsolicited phone calls or emails from a merchant
- Read merchant's refund and exchange policy before making purchase
- Do not share your password
- Always print and keep the order confirmation document
- Read the privacy statement
- Use an anti-virus, anti-spyware and personal firewall and keep it updated
- Never enter your personal information in a pop-up screen

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

CyberSecurity MALAYSIA

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 |

SAFE ONLINE BANKING

- Keep your password/PIN code safe and memorize them
- Check that the Online Banking website is secured
- Log out immediately after you have completed your online transaction
- Use an anti-virus, anti-spyware and personal firewall and keep it updated
- Do not copy or click on any links attached in emails
- Do not respond to emails asking for personal information
- Read privacy and policy information before conducting any transactions
- Check your account statements to ensure that no unauthorized transaction has taken place
- When visiting your online banking site, always check that the Date and Time, matches the date and time when you last signed in

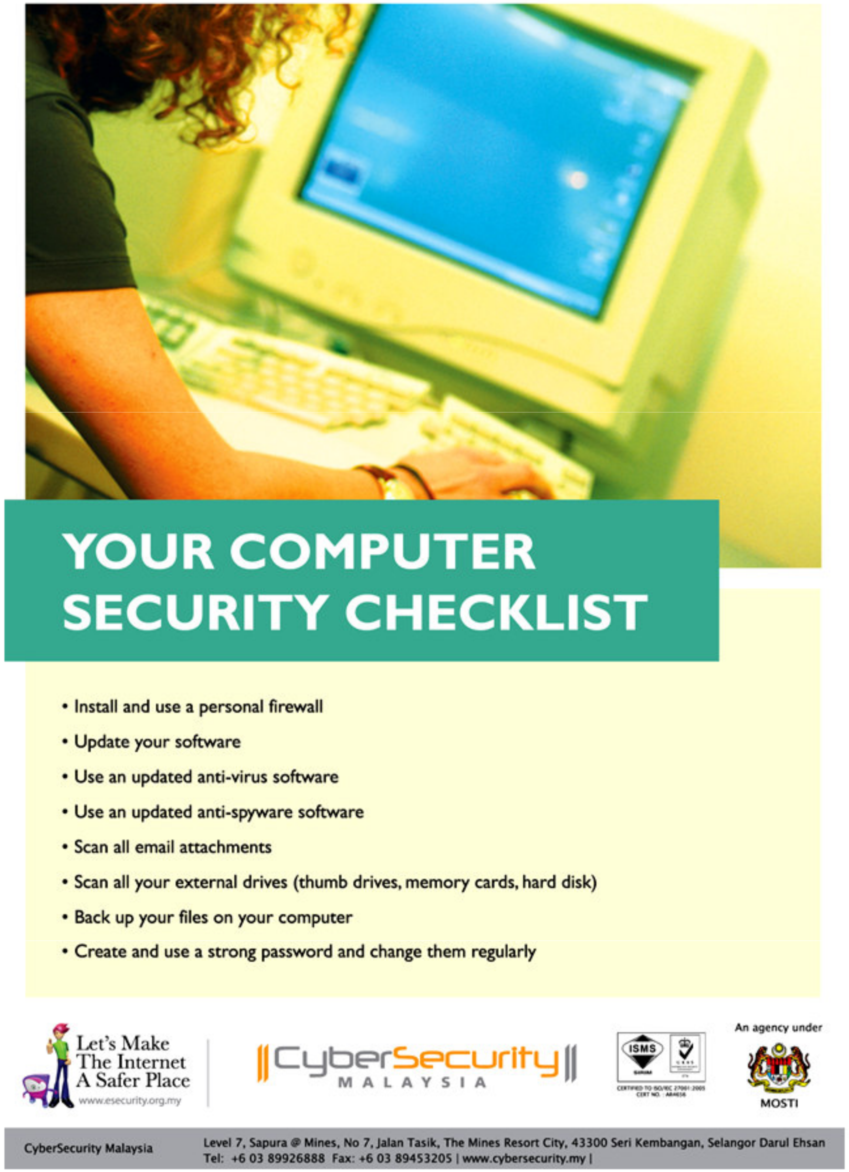
Let's Make The Internet A Safer Place
www.esecurity.org.my

CyberSecurity MALAYSIA

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

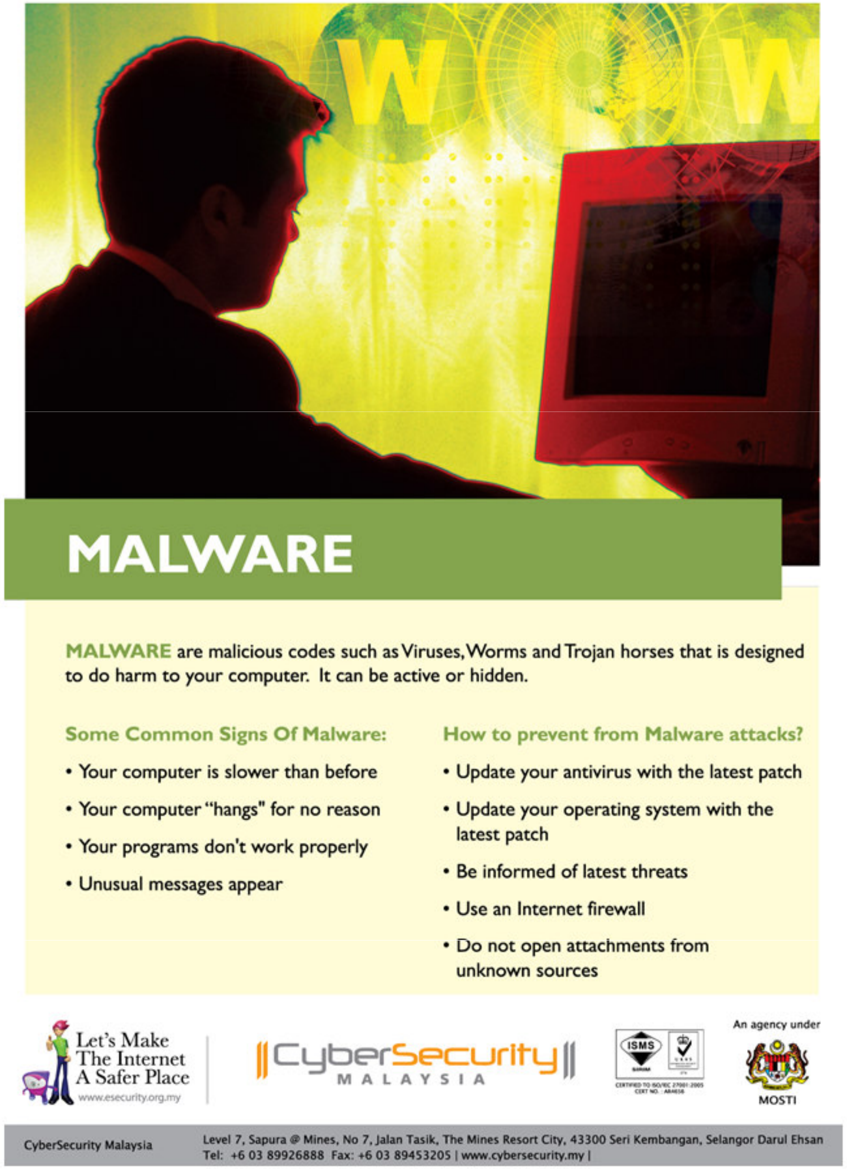


YOUR COMPUTER SECURITY CHECKLIST

- 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:

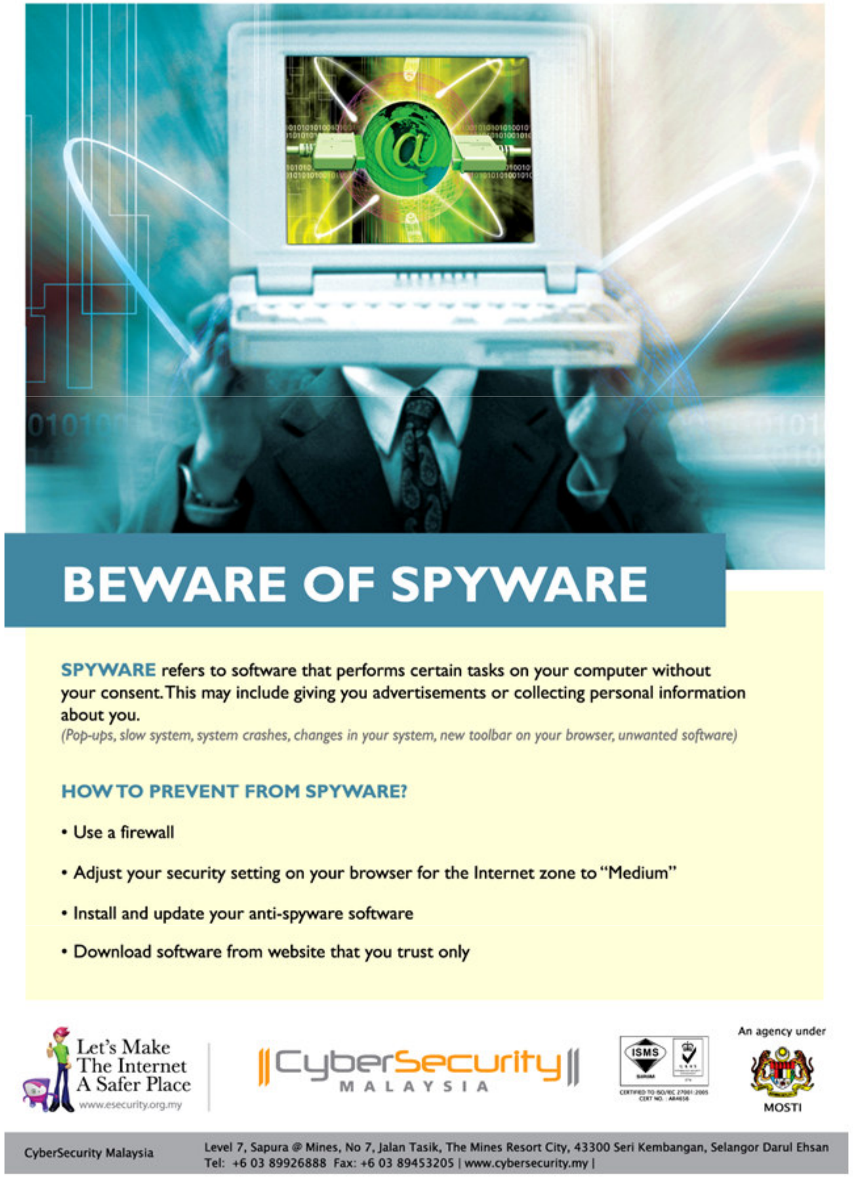
- Your computer is slower than before
- Your computer "hangs" for no reason
- Your programs don't work properly
- Unusual messages appear

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

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 |

Spyware & Password Protection



BEWARE OF SPYWARE

SPYWARE refers to software that performs certain tasks on your computer without your consent. This may include giving you advertisements or collecting personal information about you.

(Pop-ups, slow system, system crashes, changes in your system, new toolbar on your browser, unwanted software)

HOW TO PREVENT FROM SPYWARE?

- Use a firewall
- Adjust your security setting on your browser for the Internet zone to "Medium"
- Install and update your anti-spyware software
- Download software from website that you trust only

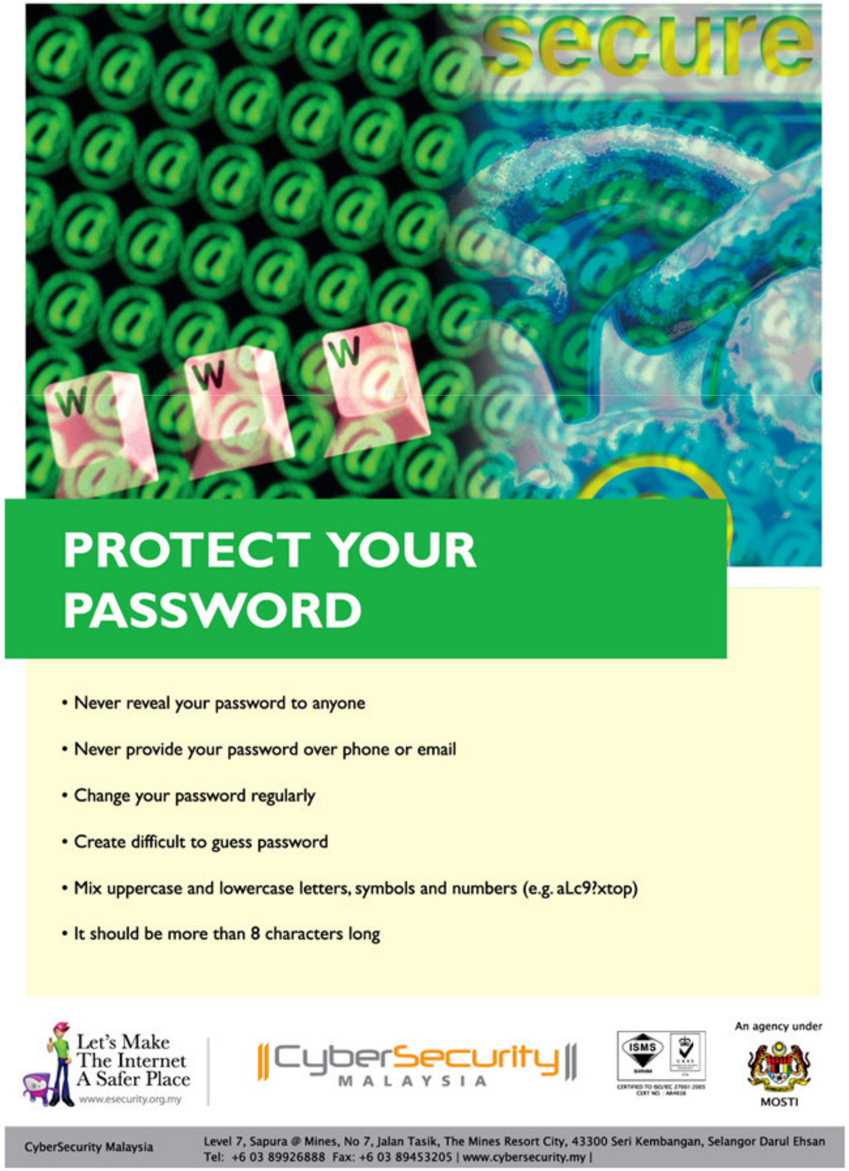
Let's Make The Internet A Safer Place
www.esecurity.org.my

CyberSecurity MALAYSIA

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 |



PROTECT YOUR PASSWORD

- Never reveal your password to anyone
- Never provide your password over phone or email
- Change your password regularly
- Create difficult to guess password
- Mix uppercase and lowercase letters, symbols and numbers (e.g. aLc9?xtop)
- It should be more than 8 characters long

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

CyberSecurity MALAYSIA

An agency under MOSTI

CyberSecurity Malaysia

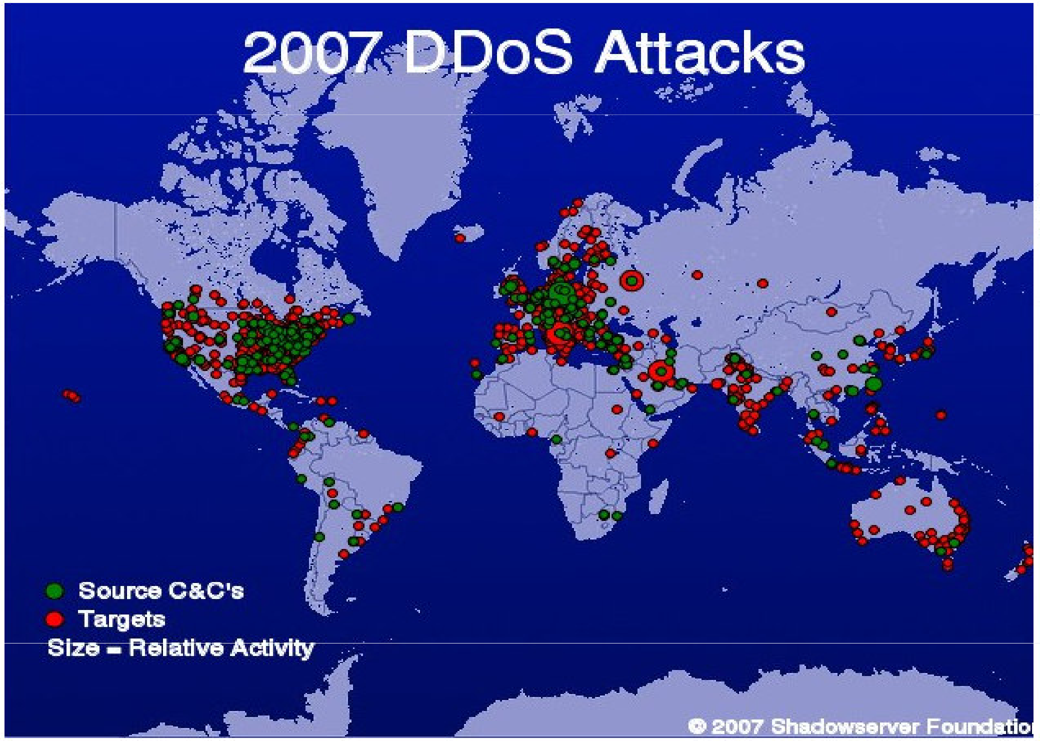
Level 7, Sapura @ Mines, No 7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan
Tel: +6 03 89926888 Fax: +6 03 89453205 | www.cybersecurity.my |

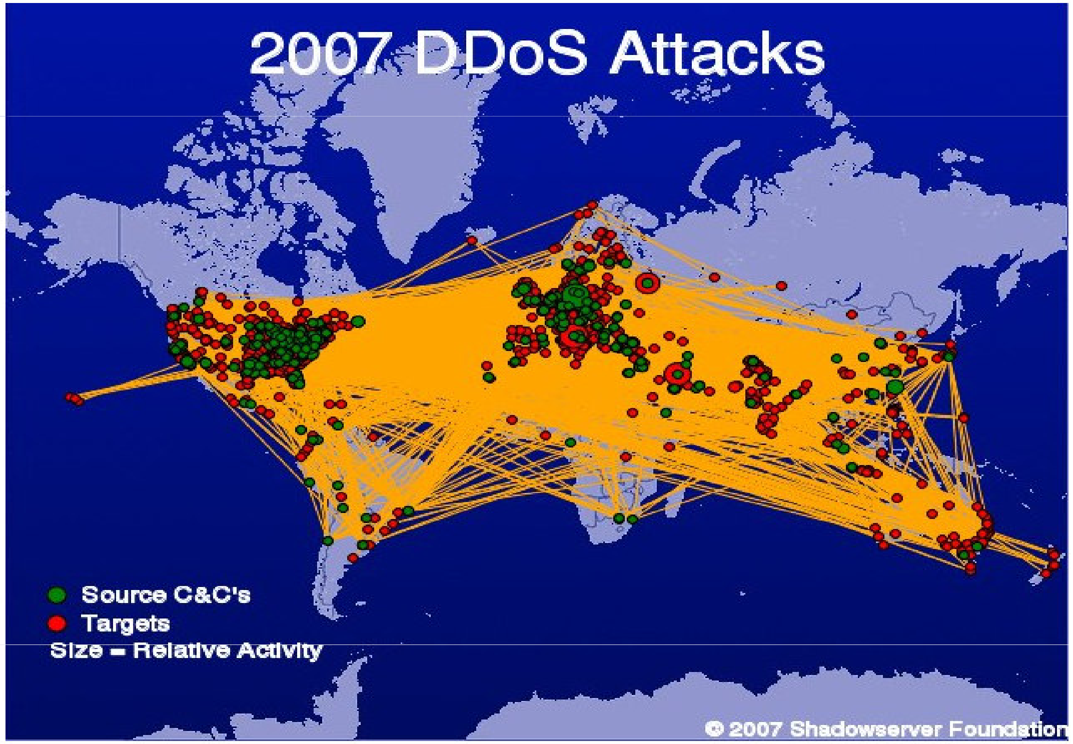
* Workshop Session 1 *

“The International Cybercrime and Cybersecurity Challenge”

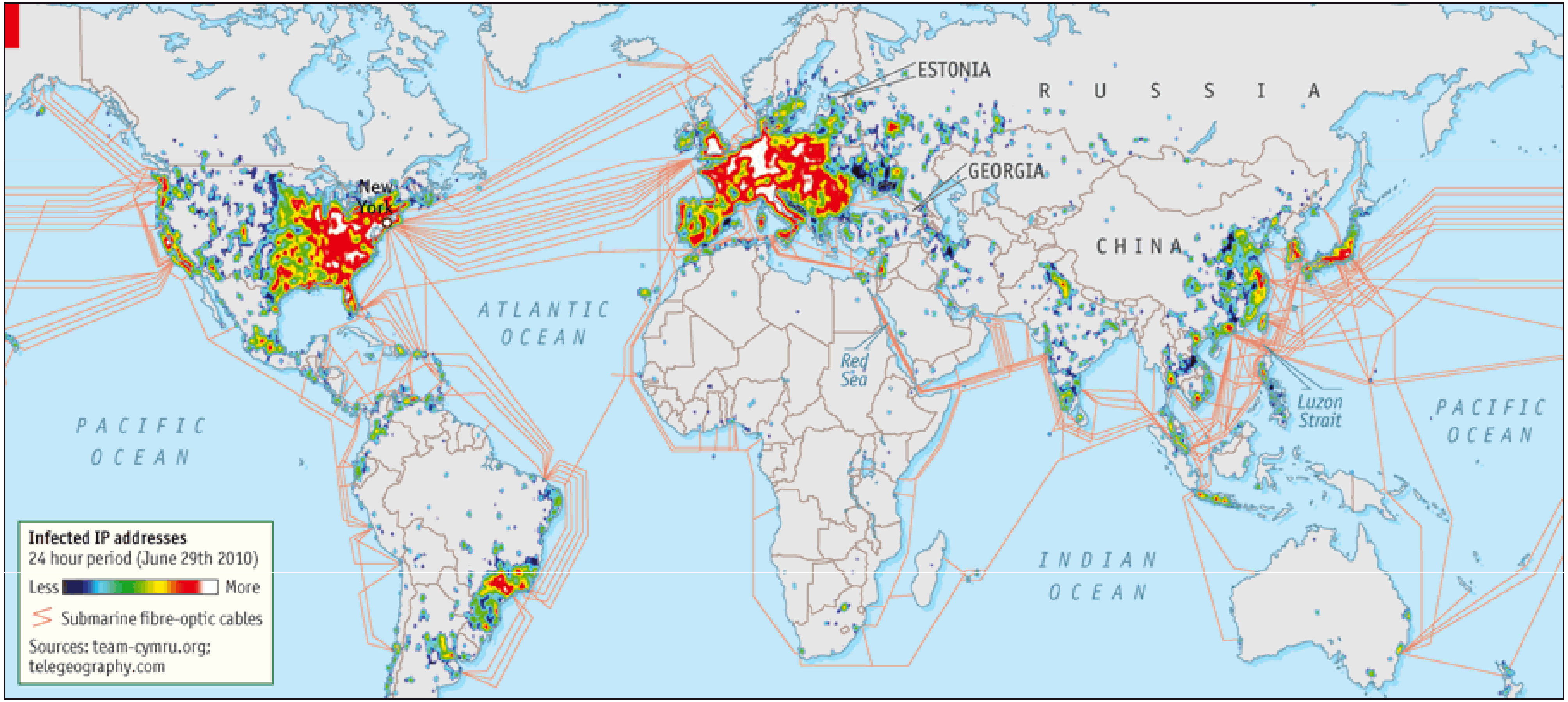
1 –Aim: National Cybersecurity	2 – Review Strategy & Plans	3 – Cyber Threats & Crimes
4 – Cyber Technical Threats	5 – Operational Security	6 – Critical Economic Sectors
7 – Case Study: Governments	8 – Case Study: Banks/Finance	9 – Key Jamaican Sectors

Global DDOS Cyberattacks - 2007

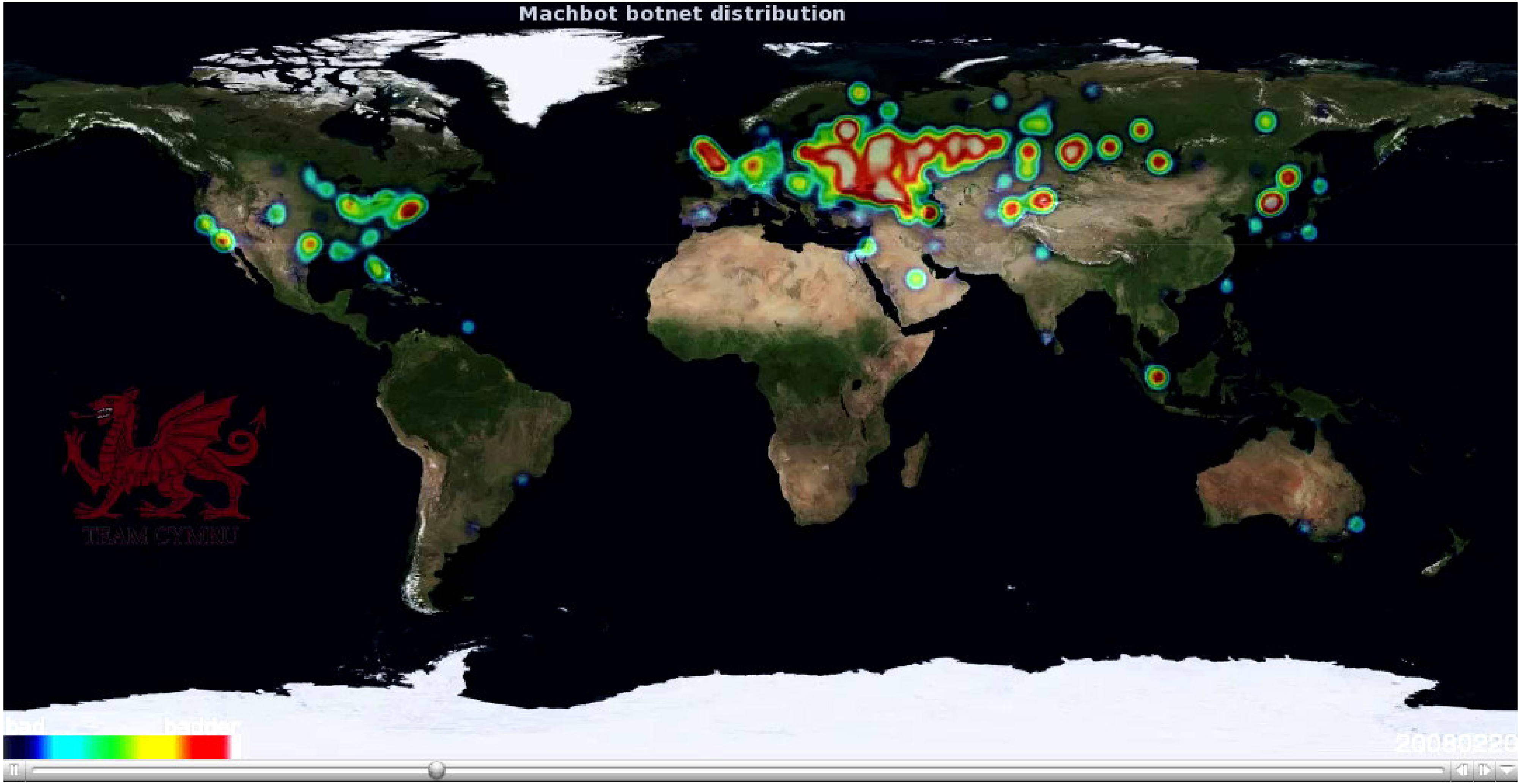




Global IP Connectivity: *Real-Time Infection*

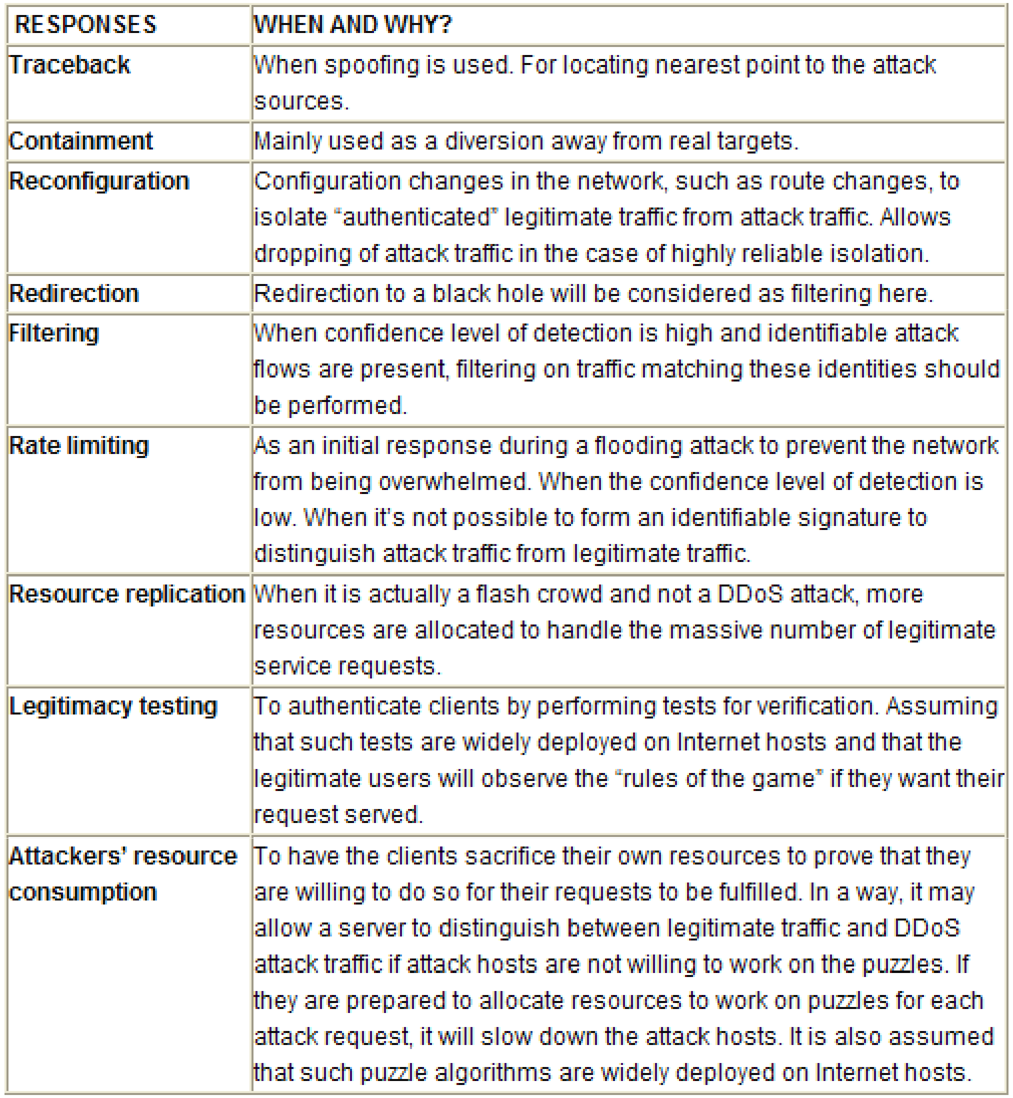


Machbot Botnet Distribution: "Team-Cymru"



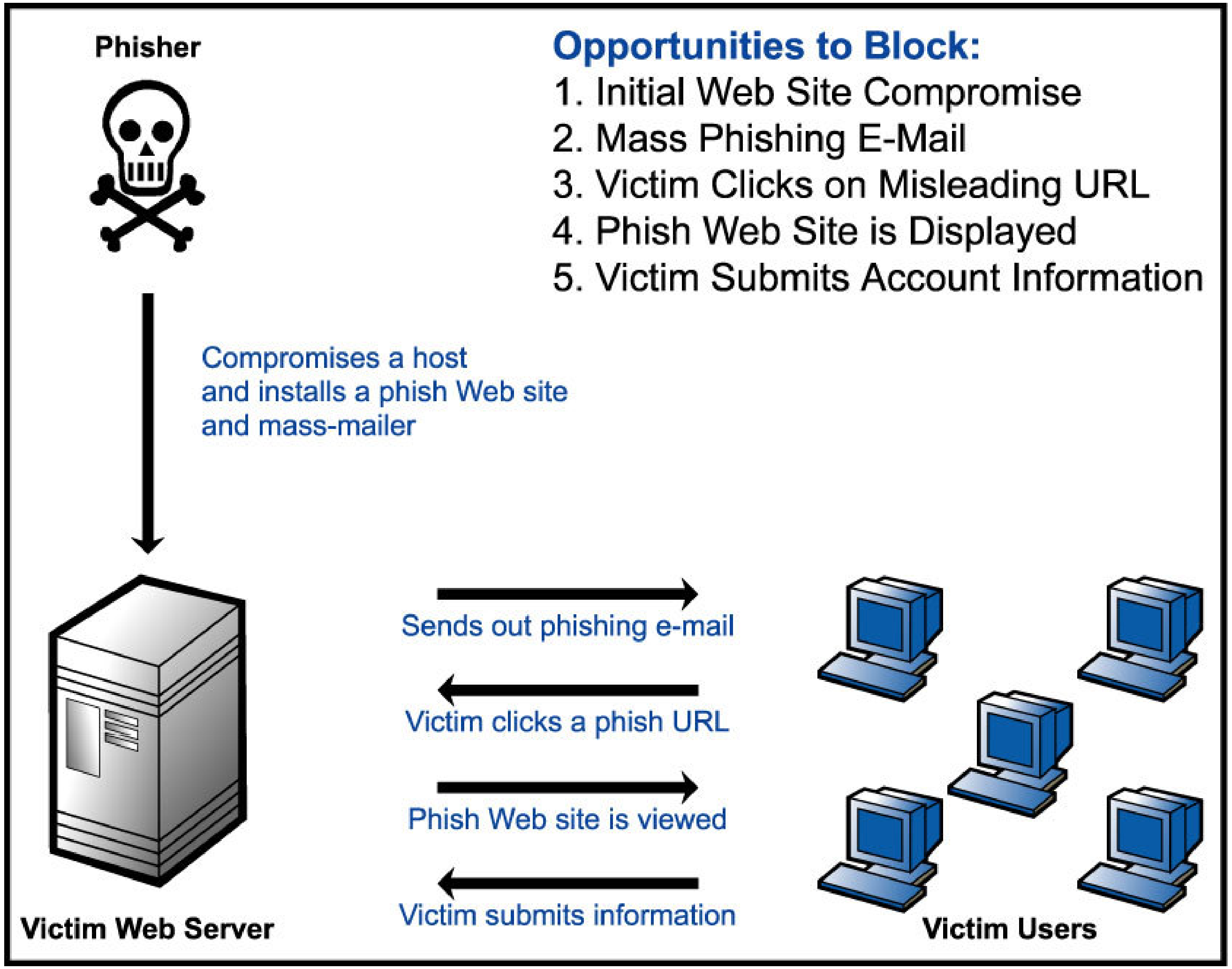
Link: www.team-cymru.org

Responses to Mitigate DDOS Attacks



RESPONSES	WHEN AND WHY?
Traceback	When spoofing is used. For locating nearest point to the attack sources.
Containment	Mainly used as a diversion away from real targets.
Reconfiguration	Configuration changes in the network, such as route changes, to isolate "authenticated" legitimate traffic from attack traffic. Allows dropping of attack traffic in the case of highly reliable isolation.
Redirection	Redirection to a black hole will be considered as filtering here.
Filtering	When confidence level of detection is high and identifiable attack flows are present, filtering on traffic matching these identities should be performed.
Rate limiting	As an initial response during a flooding attack to prevent the network from being overwhelmed. When the confidence level of detection is low. When it's not possible to form an identifiable signature to distinguish attack traffic from legitimate traffic.
Resource replication	When it is actually a flash crowd and not a DDoS attack, more resources are allocated to handle the massive number of legitimate service requests.
Legitimacy testing	To authenticate clients by performing tests for verification. Assuming that such tests are widely deployed on Internet hosts and that the legitimate users will observe the "rules of the game" if they want their request served.
Attackers' resource consumption	To have the clients sacrifice their own resources to prove that they are willing to do so for their requests to be fulfilled. In a way, it may allow a server to distinguish between legitimate traffic and DDoS attack traffic if attack hosts are not willing to work on the puzzles. If they are prepared to allocate resources to work on puzzles for each attack request, it will slow down the attack hosts. It is also assumed that such puzzle algorithms are widely deployed on Internet hosts.

Phishing Attack: Typical Process



Phisher

Opportunities to Block:

1. Initial Web Site Compromise
2. Mass Phishing E-Mail
3. Victim Clicks on Misleading URL
4. Phish Web Site is Displayed
5. Victim Submits Account Information

Compromises a host and installs a phish Web site and mass-mailer

Sends out phishing e-mail

Victim clicks a phish URL

Phish Web site is viewed

Victim submits information

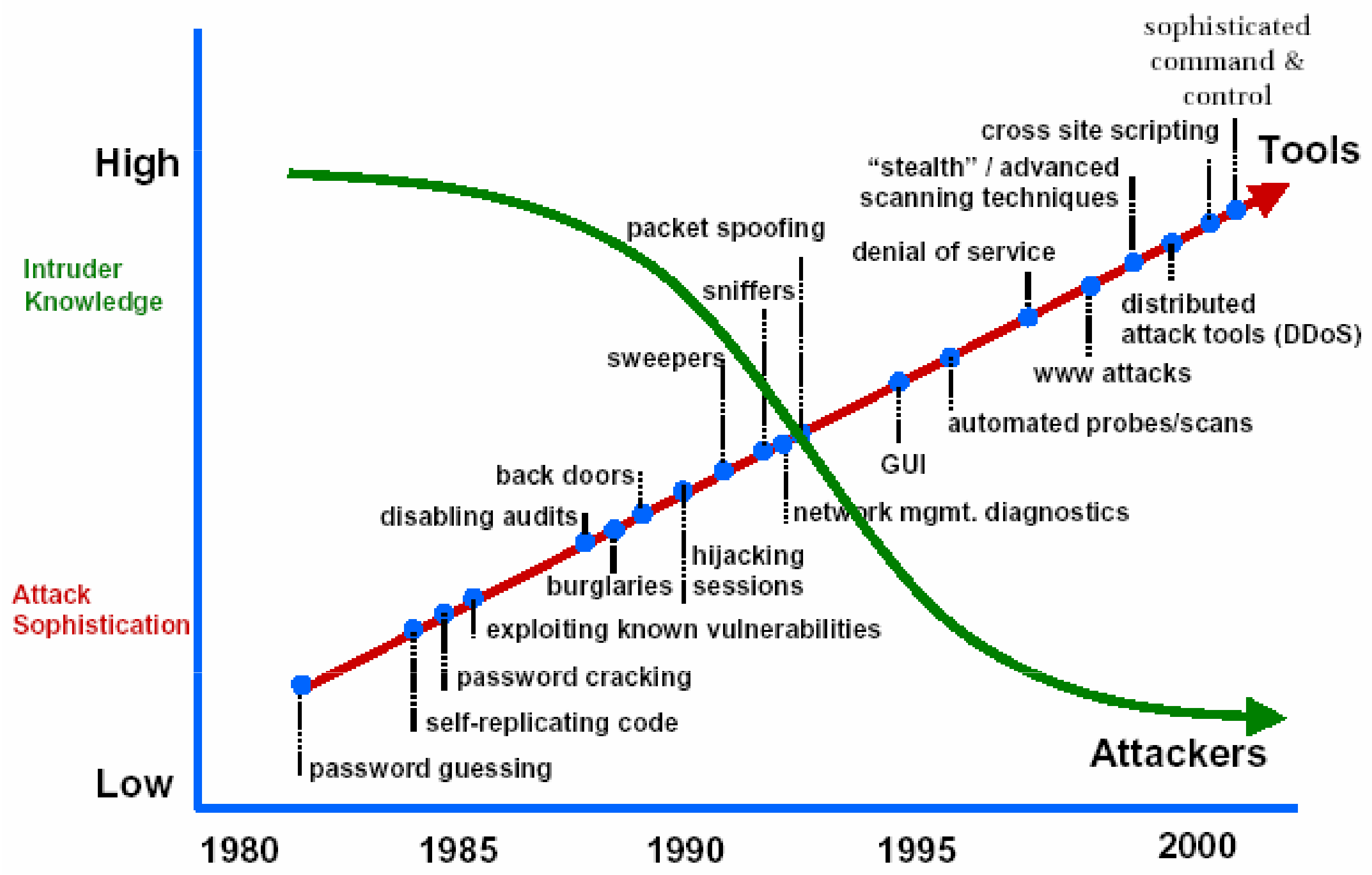
Victim Web Server

Victim Users

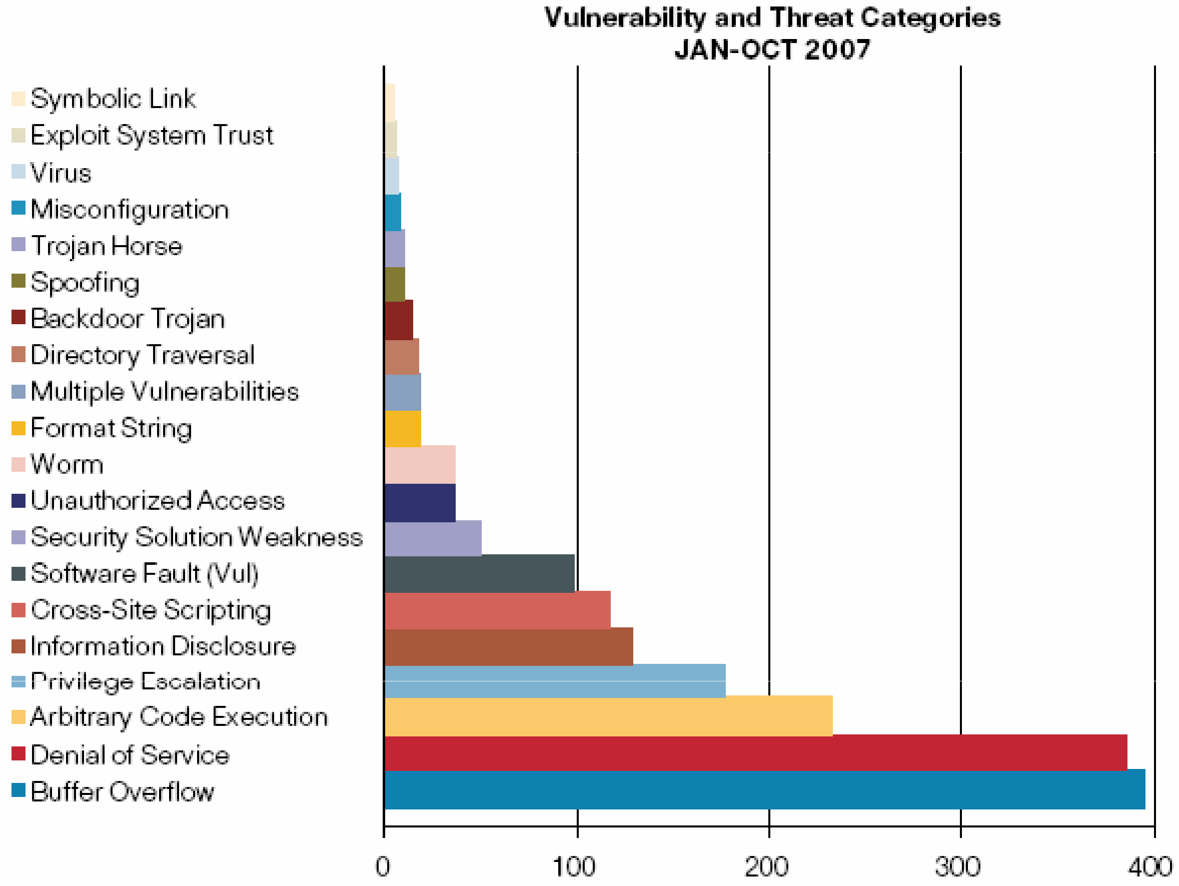
Technical Cyber Threats

1) Phishing Scams such as Advance Fee & Lottery Scams
2) Spam eMail with malicious intent
3) DDOS Denial of Service "Botnet" Attacks
4) SQL Database Injection
5) XSS Cross-Scripting Java Script Attacks
6) Personal Identity Theft (ID Theft)
7) Malware, Spyware, Worms, Viruses & Trojans
8) Embedded *Sleeping* Software "Zombie Bots"
9) Buffer Overflow Attacks
10) Firewall Port Scanners
11) Social Networking "Malware Apps"
12) Wi-Fi, Bluetooth & Mobile Network Intrusion
13) Keyloggers – Hardware and Software Variants

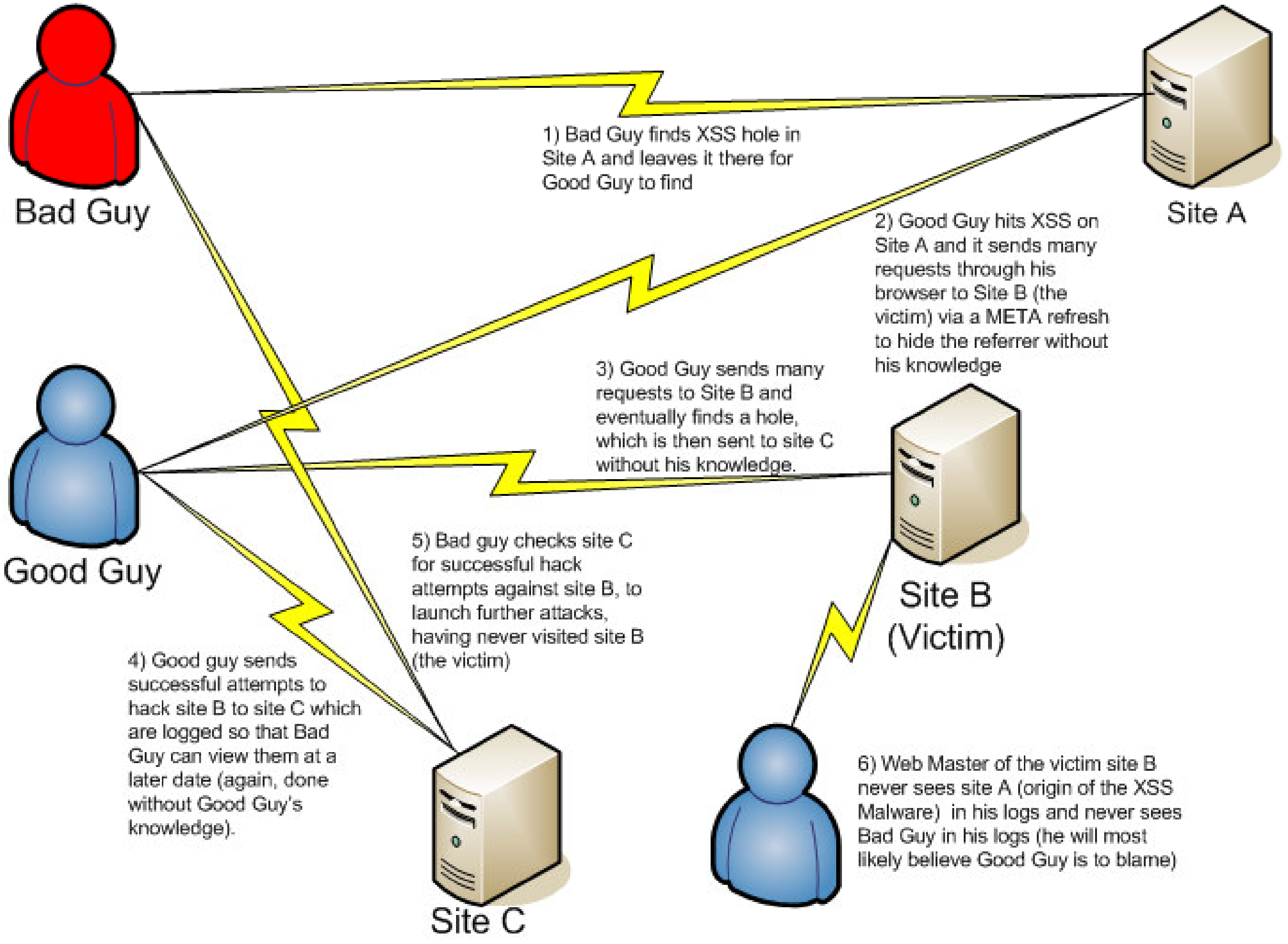
Attacker Sophistication vs Intruder Technical Knowledge



Top 20 Threats and Vulnerabilities - 2007



Cross-Site Scripting by Proxy : XSS



1) Bad Guy finds XSS hole in Site A and leaves it there for Good Guy to find

2) Good Guy hits XSS on Site A and it sends many requests through his browser to Site B (the victim) via a META refresh to hide the referrer without his knowledge

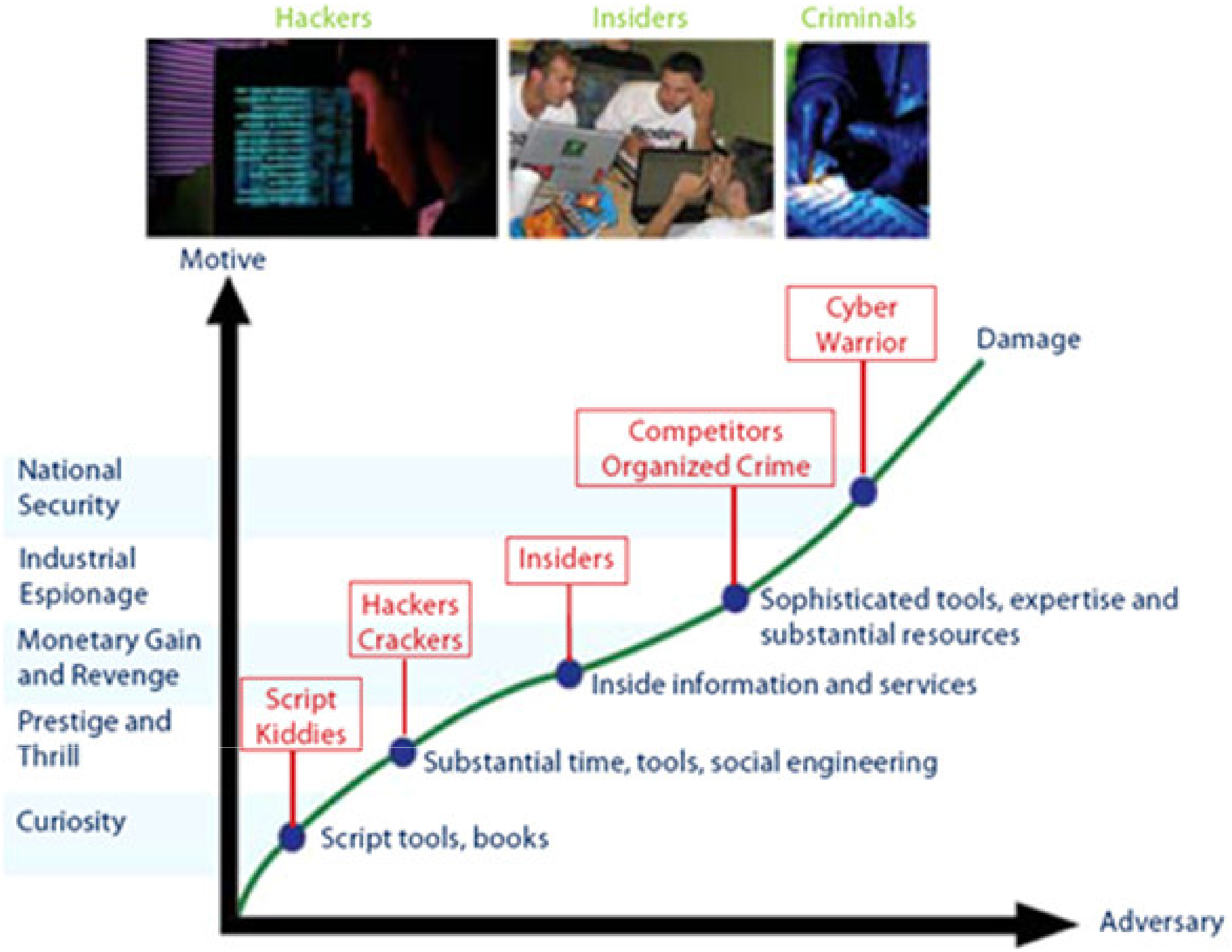
3) Good Guy sends many requests to Site B and eventually finds a hole, which is then sent to site C without his knowledge.

4) Good guy sends successful attempts to hack site B to site C which are logged so that Bad Guy can view them at a later date (again, done without Good Guy's knowledge).

5) Bad guy checks site C for successful hack attempts against site B, to launch further attacks, having never visited site B (the victim)

6) Web Master of the victim site B never sees site A (origin of the XSS Malware) in his logs and never sees Bad Guy in his logs (he will most likely believe Good Guy is to blame)

Hierarchy of Hacking Skills



Hackers
Insiders
Criminals
Motive
National Security
Industrial Espionage
Monetary Gain and Revenge
Prestige and Thrill
Curiosity
Cyber Warrior
Damage
Competitors Organized Crime
Insiders
Hackers Crackers
Script Kiddies
Sophisticated tools, expertise and substantial resources
Inside information and services
Substantial time, tools, social engineering
Script tools, books
Adversary

Underground Cyber Economy

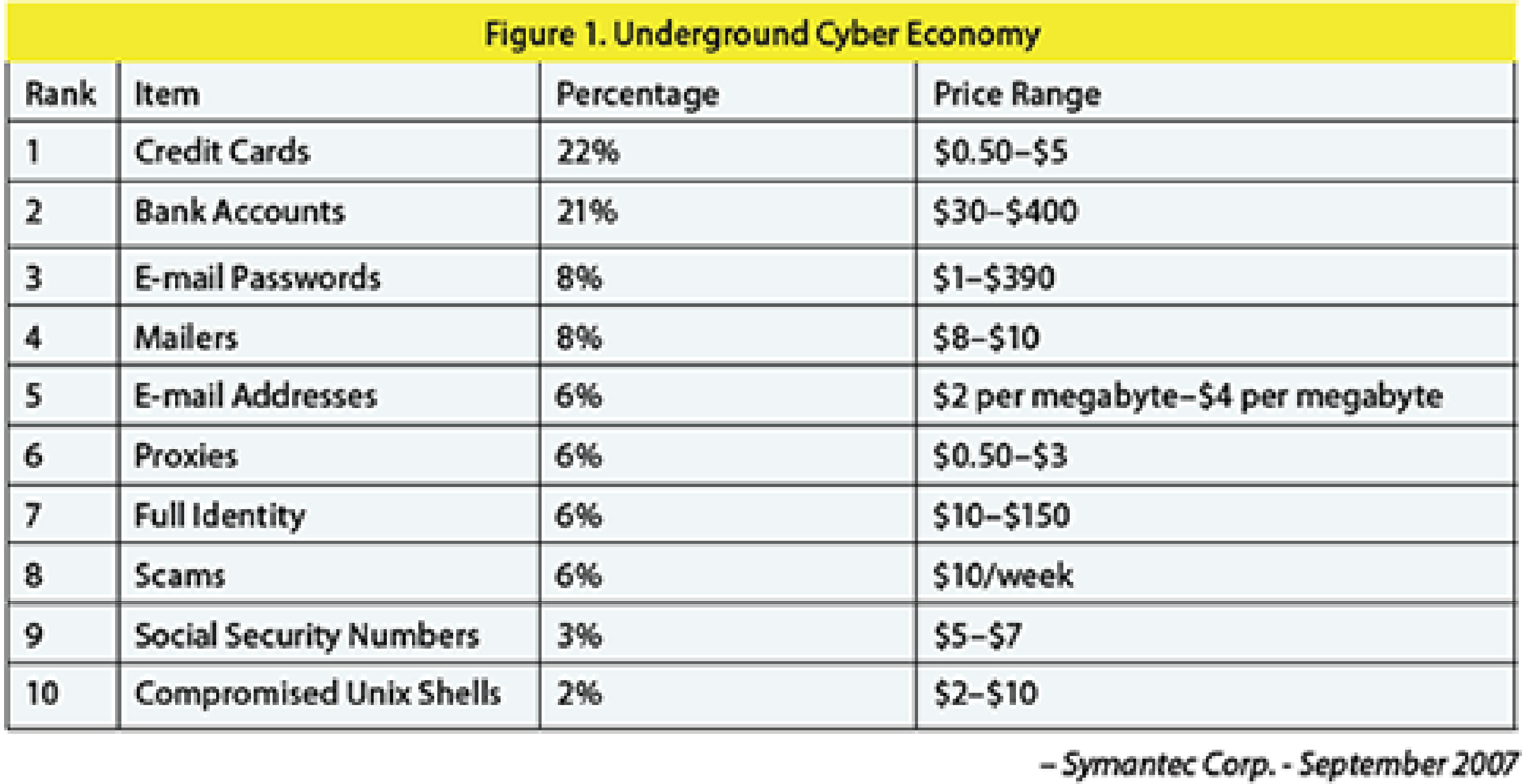


Figure 1. Underground Cyber Economy

Rank	Item	Percentage	Price Range
1	Credit Cards	22%	$0.50–$5
2	Bank Accounts	21%	$30–$400
3	E-mail Passwords	8%	$1–$390
4	Mailers	8%	$8–$10
5	E-mail Addresses	6%	$2 per megabyte–$4 per megabyte
6	Proxies	6%	$0.50–$3
7	Full Identity	6%	$10–$150
8	Scams	6%	$10/week
9	Social Security Numbers	3%	$5–$7
10	Compromised Unix Shells	2%	$2–$10

– Symantec Corp. - September 2007

* Workshop Session 1 *

"The International Cybercrime and Cybersecurity Challenge"

1 –Aim: National Cybersecurity	2 – Review Strategy & Plans	3 – Cyber Threats & Crimes
4 – Cyber Technical Threats	5 – Operational Security	6 – Critical Economic Sectors
7 – Case Study: Governments	8 – Case Study: Banks/Finance	9 – Key Jamaican Sectors

Operational Security Threats

1) *Access:* Campus, Building and ICT Facility Access
2) *Staff:* Facility Staff, Contractors and Visitors
3) *ID:* Forged or Stolen Access ID & Biometric Cards
4) *Lost* Laptops, Memory Sticks, Smart Phones & Storage Drives
5) *Stolen* Information & Data Assets, both physical & electronic
6) *Wireless:* Personal Wireless and Bluetooth Access Points
7) *Perimeter* Fencing for Critical Facilities: Airports, Power Stations
8) *Vehicles:* Criminal or Terrorist Vehicles parked with Fake Plates
9) *Compliance:* Non-Compliance with operational security policies
10) *Training:* Superficial training for cyber events, alarms & emergencies

……..We'll be considering the operational security solutions to all these threats during these 2 days, and their integration with cybersecurity.

* Workshop Session 1 *

“The International Cybercrime and Cybersecurity Challenge”

1 –Aim: National Cybersecurity	2 – Review Strategy & Plans	3 – Cyber Threats & Crimes
4 – Cyber Technical Threats	5 – Operational Security	6 – Critical Economic Sectors
7 – Case Study: Governments	8 – Case Study: Banks/Finance	9 – Key Jamaican Sectors

Critical Economic Service Sectors

- During our 2-day workshop we shall consider the specific security requirements for each of the major critical sectors including:

1) *Government:* Protection against criminal & terrorist threats and attacks
2) *Banking/Finance:* Protection against cybercriminals & money laundering
3) *Healthcare:* Security of the hospitals, medical records and equipment
4) *Telecommunications:* Security of comms links, data, servers & facilities
5) *National & Civil Defence* : Protection of military & police info and assets
6) *Energy & Water Utilities*: Security of the power grid and water supplies
7) *Education*: Security of the Universities, Schools and College Campuses
8) *Transportation & Ports* : Airport & Ports Security against Crime & Terrorists
9) *Tourism* : Hotel and Resort Security for Guests and Staff
10) *Emergency Services*: Security of Integrated Communications

* Workshop Session 1 *

“The International Cybercrime and Cybersecurity Challenge”

1 –Aim: National Cybersecurity	2 – Review Strategy & Plans	3 – Cyber Threats & Crimes
4 – Cyber Technical Threats	5 – Operational Security	6 – Critical Economic Sectors
7 – Case Study: Governments	8 – Case Study: Banks/Finance	9 – Key Jamaican Sectors

Sector Case Study: Governments

- *Cyber Agencies:* Governments such as UK, USA, Malaysia, South Korea and Australia have all implemented cybersecurity agencies & programmes
- *eGovernment Services* are critically dependant upon strong cybersecurity for the protection of applications, and citizen data
- *Compliance Audit:* All Government Ministries & Agencies should receive in-depth ICT security audits, as well as full annual compliance reviews

1) National Defence Forces
2) Parliamentary Resources
3) Land Registry & Planning System
4) Citizen IDs and Passports
5) Laws, Legislations, and Policies
6) Civilian Police, Prisons & National e-Crimes Unit (NCU)
7) National CERT – Computer Emergency Response Team
8) Inter-Government Communications Network
9) eServices for Regional & International Partnerships
10) Establishment of cybersecurity standards & compliance
11) Government Security Training and Certification

* Workshop Session 1 *

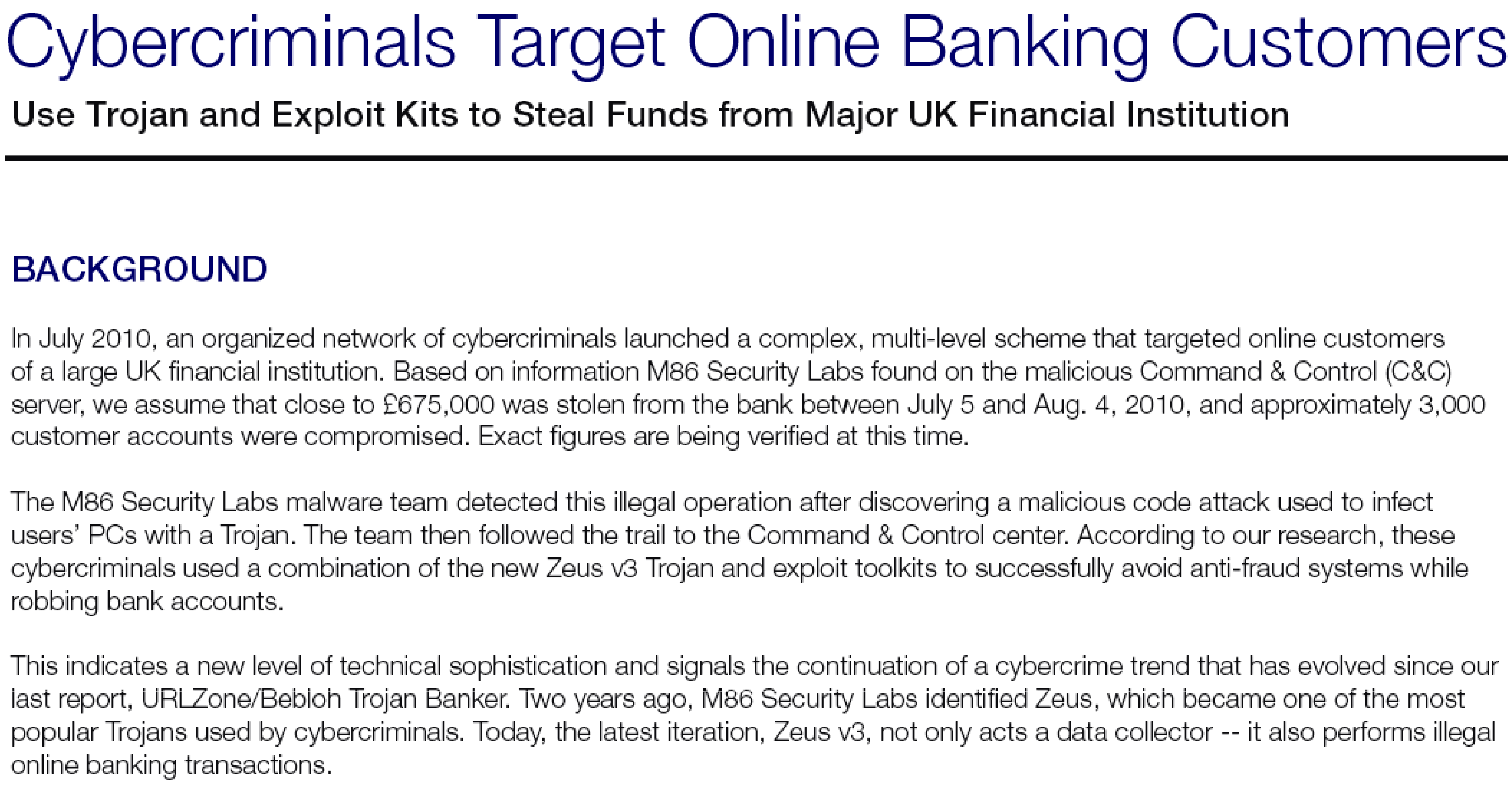
“The International Cybercrime and Cybersecurity Challenge”

1 –Aim: National Cybersecurity	2 – Review Strategy & Plans	3 – Cyber Threats & Crimes
4 – Cyber Technical Threats	5 – Operational Security	6 – Critical Economic Sectors
7 – Case Study: Governments	8 – Case Study: Banks/Finance	9 – Key Jamaican Sectors

Sector Case Study: Banks & Finance

- *Banks & Financial* Institutions are prime targets for cybercriminals.
- *Access* to Accounts is usually indirect through phishing scams, infected websites with malicious scripts, and personal ID Theft.
- *On-Line bank transfers* are also commonly used for international money laundering of funds secured from illegal activities
- *Instant Money Transfer Services* are preferred for crimes such as the classic "Advanced Fee Scam" as well as Lottery and Auction Scams
- An increasing problem is *Cyber-Extortion* instigated through phishing
- *National & Commercial Ban*ks have also been targets of DDOS cyberattacks from politically motivated and terrorist organisations
- *Penetration Scans:* Banks are pivotal to national economies and will receive penetration scans and attempted hacks on a regular basis.
- *On-Line Banking* networks including ATMs, Business and Personal Banking are at the "sharp end" of financial security and require great efforts towards end-user authentication & transaction network security

Cybercriminals Target UK Bank: July 2010



Cybercriminals Target Online Banking Customers

Use Trojan and Exploit Kits to Steal Funds from Major UK Financial Institution

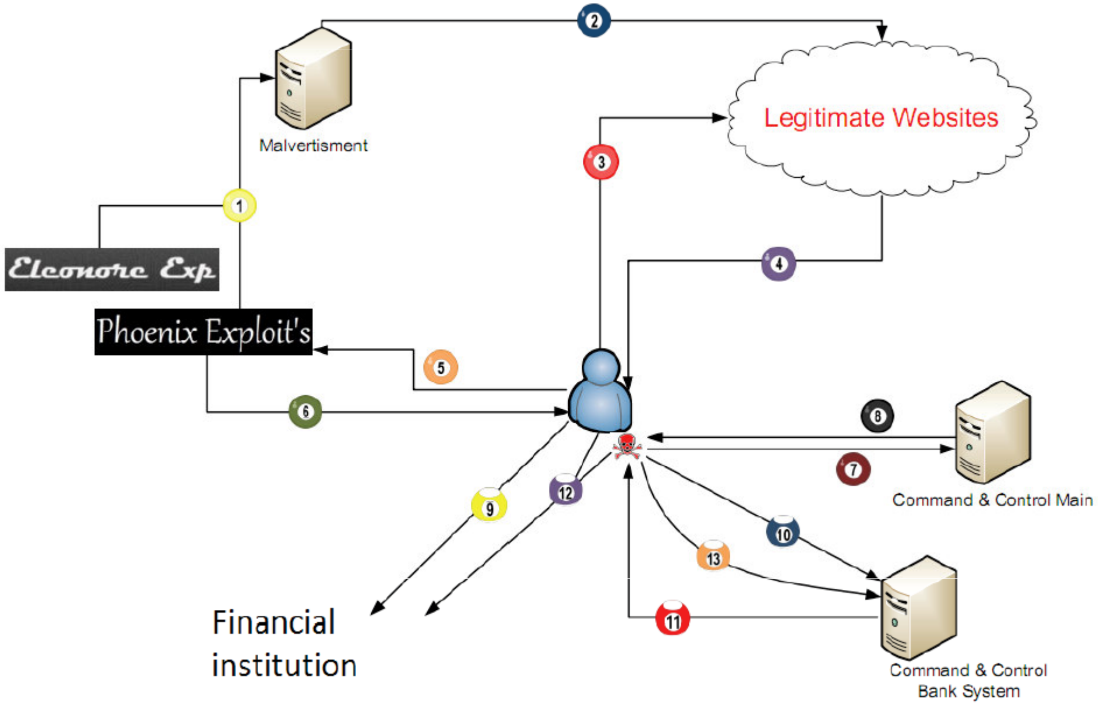
BACKGROUND

In July 2010, an organized network of cybercriminals launched a complex, multi-level scheme that targeted online customers of a large UK financial institution. Based on information M86 Security Labs found on the malicious Command & Control (C&C) server, we assume that close to £675,000 was stolen from the bank between July 5 and Aug. 4, 2010, and approximately 3,000 customer accounts were compromised. Exact figures are being verified at this time.

The M86 Security Labs malware team detected this illegal operation after discovering a malicious code attack used to infect users' PCs with a Trojan. The team then followed the trail to the Command & Control center. According to our research, these cybercriminals used a combination of the new Zeus v3 Trojan and exploit toolkits to successfully avoid anti-fraud systems while robbing bank accounts.

This indicates a new level of technical sophistication and signals the continuation of a cybercrime trend that has evolved since our last report, URLZone/Bebloh Trojan Banker. Two years ago, M86 Security Labs identified Zeus, which became one of the most popular Trojans used by cybercriminals. Today, the latest iteration, Zeus v3, not only acts a data collector -- it also performs illegal online banking transactions.

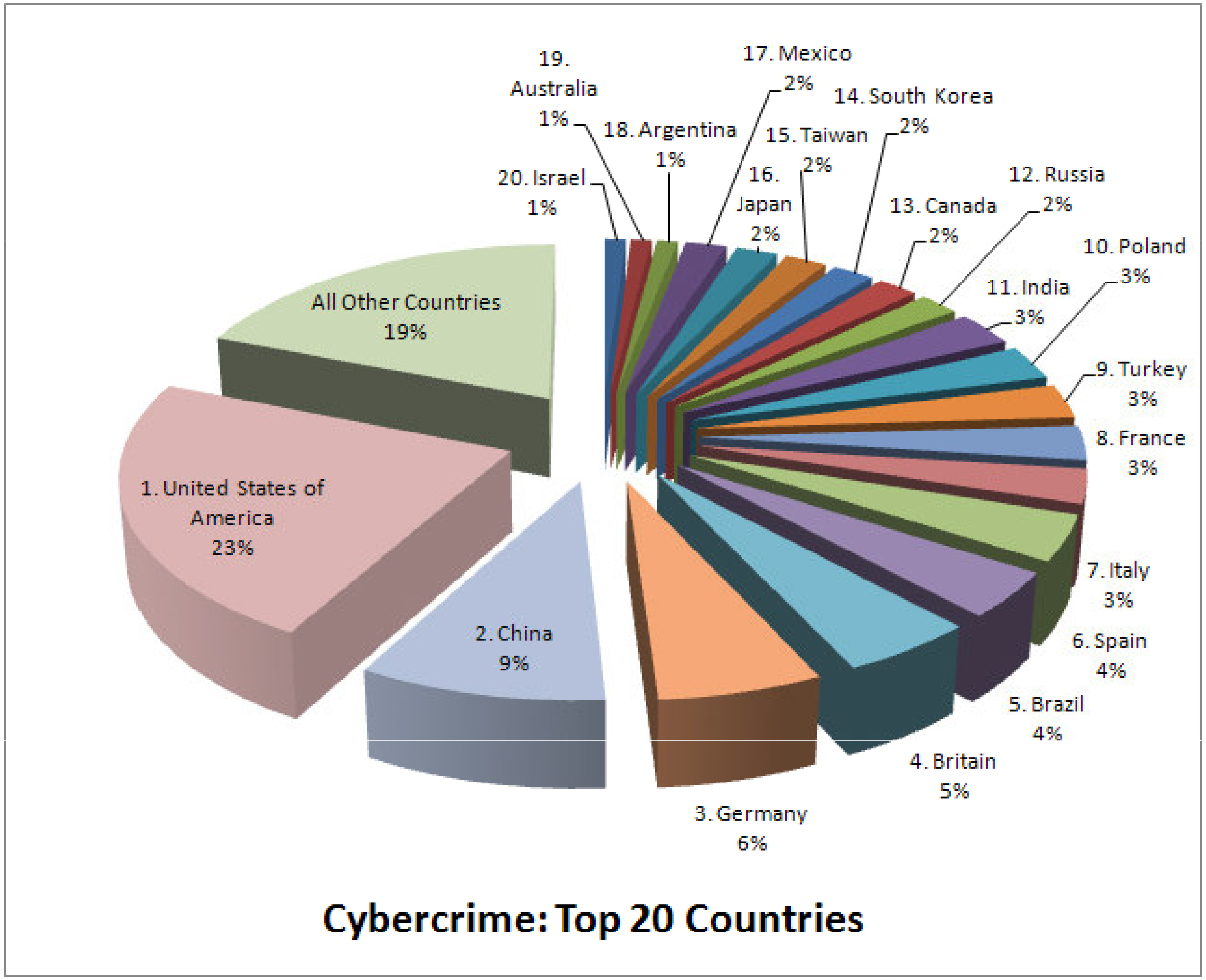
Process Flow of the Cybercriminal Attack on UK Financial Institution: July/August 2010



1. Uploads malicious advertisements to legitimate and fraud advertisements servers
2. The malicious advertisements published among the legitimate websites
3. User accesses to an infected website
4. The website content contains redirection to the malicious Exploit Kit
5. The user is redirected to the malicious Exploit Kit
6. The user's PC exploited, the payload was downloaded successfully
7. The Trojan reports for a new bot to the C&C
8. The C&C sends instruction to the Trojan
9. User access to financial institution
10. The Trojan reports for the user activities
11. The C&C sends commands to the Trojan to manipulate user bank transactions
12. Trojan manipulates User's bank transaction
13. Trojan reports the C&C about successful/failed transaction

Source: White Paper by M86 Security: Aug 2010

Cybercrime: Top 20 Countries



University of Technology, Jamaica

International Telecommunication Union

Committed to connecting the world

* Workshop Session 1 *

“The International Cybercrime and Cybersecurity Challenge”

1 –Aim: National Cybersecurity	2 – Review Strategy & Plans	3 – Cyber Threats & Crimes
4 – Cyber Technical Threats	5 – Operational Security	6 – Critical Economic Sectors
7 – Case Study: Governments	8 – Case Study: Banks/Finance	9 – Key Jamaican Sectors

Cybersecurity for Key Jamaican Sectors

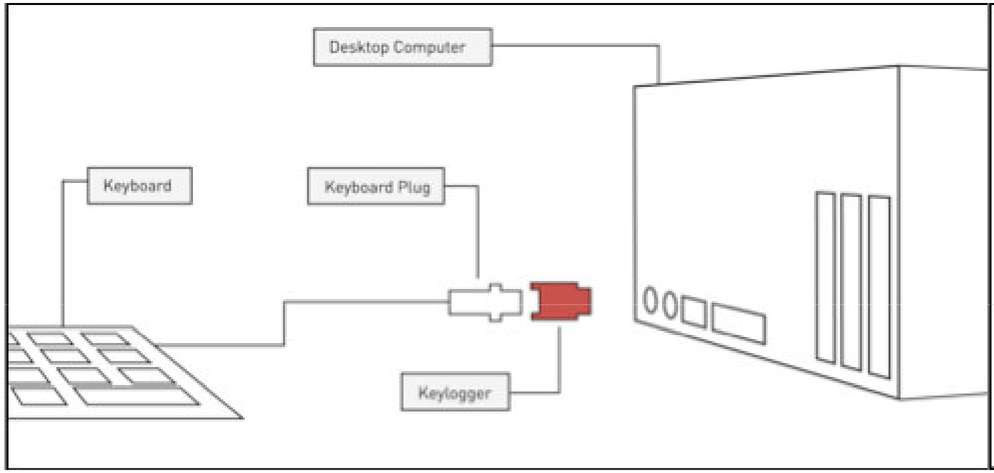
- During the last 5 years, cybercrime has become a major political and business issue for the Jamaican Government and Enterprises.

- The key sectors that we'll be analysing, as a group, for technical & operational solutions within the Jamaican Economy will be:

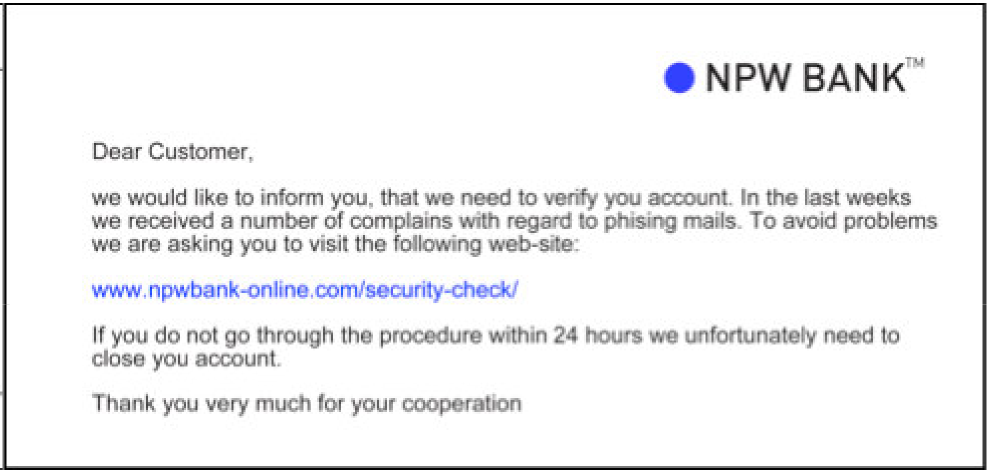
  - Banking/Financial Sector
  - International Airports & Ports (Kingston & Montego Bay)
  - Police Force and Cybercrime Unit
  - Telecomms, ISP & Mobile Sector
  - Travel/Tourism Sector
  - Import/Export Trade
  - Educational Sector

…..In the next session we'll explore generic cybersecurity & operational security solutions, and their practical integration in real-world organisations

Typical Cybercrime Threats



(a) – Hardware & Software Keyloggers


NPW BANK™

Dear Customer,

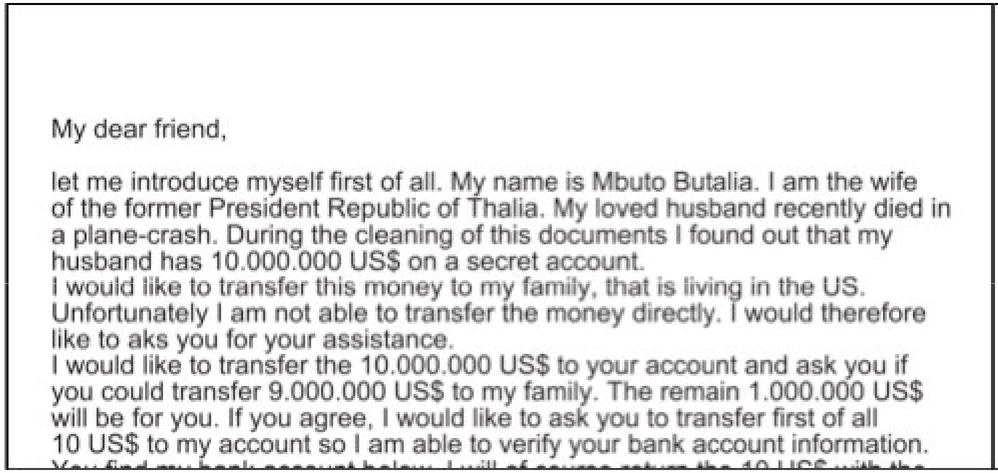
we would like to inform you, that we need to verify you account. In the last weeks we received a number of complains with regard to phising mails. To avoid problems we are asking you to visit the following web-site:

www.npwbank-online.com/security-check/

If you do not go through the procedure within 24 hours we unfortunately need to close you account.

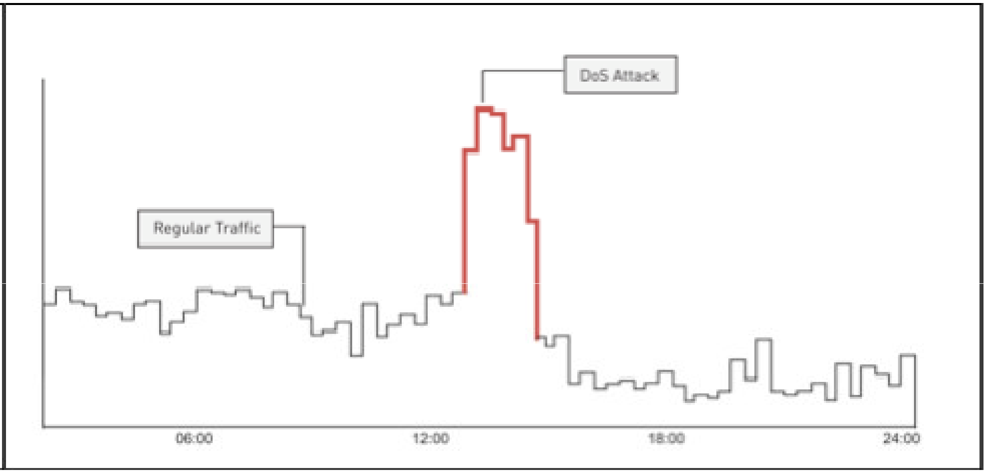
Thank you very much for your cooperation

(b) – Email Phishing


My dear friend,

let me introduce myself first of all. My name is Mbuto Butalia. I am the wife of the former President Republic of Thalia. My loved husband recently died in a plane-crash. During the cleaning of this documents I found out that my husband has 10.000.000 US$ on a secret account.
I would like to transfer this money to my family, that is living in the US. Unfortunately I am not able to transfer the money directly. I would therefore like to aks you for your assistance.
I would like to transfer the 10.000.000 US$ to your account and ask you if you could transfer 9.000.000 US$ to my family. The remain 1.000.000 US$ will be for you. If you agree, I would like to ask you to transfer first of all 10 US$ to my account so I am able to verify your bank account information.
You find my bank account below. I will of course return the 10 US$ with the

(c) – Advance Fee Scam



(d) – Denial of Service

* ITU Workshop Overview*

"Cybersecurity Technologies, Standards & Operations"

S1-Thurs: 9:30-11:00 "The International Cybercrime and Cybersecurity Challenge"	S2–Thurs:11:30-13:00 "Integration Cyber-Technological Solutions for the 21stC Web2.0 World"	S3-Thurs:14:00-15:30 Group Session: "Securing Critical Computing and Network Facilities"	S4-Thurs:16:00-17:30 Group Session: "Group Discussion: Securing Critical Computing and Network Facilities"
S5 - Fri: 9:30–11:00 "Cybersecurity Continuity Planning, Standards and Architectures"	S6 – Fri: 11:30–13:00 "Organising a National Crime Unit and CERT/CSIRT"	S7 – Fri: 14:00-15:30 Group Session: "Designing Practical Cybercrime Solutions – Critical Sectors"	S7 – Fri: 16:00-17:30 Group Session" "Group Discussion: Designing Practical Cybercrime Solutions – Critical Sectors"

*Workshop Session 2 *

"Integrated Cyber-Technological Solutions for the 21stC Web2.0 World"

1 – The 21stC Cyber World	2 – ITU Global CyberAgenda	3 – Cyber Technical Solutions:A
4 – Cyber Technical Solutions:B	5–Physical Security Solutions:A	6–Physical Security Solutions:B
7 – "Cyber to Physical Attacks"	8 – "Physical to Cyber Attacks"	9–Integrated Security Benefits

*Workshop Session 2 *

"Integrated Cyber-Technological Solutions for the 21stC Web2.0 World"

1 – The 21stC Cyber World	2 – ITU Global CyberAgenda	3 – Cyber Technical Solutions:A
4 – Cyber Technical Solutions:B	5–Physical Security Solutions:A	6–Physical Security Solutions:B
7 – "Cyber to Physical Attacks"	8 – "Physical to Cyber Attacks"	9–Integrated Security Benefits

"21st Century Cyber World"

- *Open World:* During the last 15 years we've evolved from the primitive Internet to the complex world of Web2.0 applications
- *Criminals and Hackers* seek every opportunity to creatively penetrate wired, wireless, mobile devices, and social networking applications
- *The war against cybercriminals* requires us to continuously create new cybersecurity solutions for every conceivable cyberattack
- *Standards, Architectures and Operational Security Policies* all ensure that the "business case for cybercriminals" is much less attractive
- *The DMZ Security Firewalls* of the 1990s are now only a partial solution to the protection of critical information infrastructure

…….In this session we explore the 21st World of Cybersecurity Solutions including their integration with the more traditional physical security & surveillance systems………

Cybersecurity for Wireless Networks & Web2.0 "Apps"

- Wireless Networks: The open world of wireless, mobile devices & storage requires a new 21stC conceptual approach to cybersecurity:

1) *Embedded:* Security should be embedded at EVERY node of the network and applications
2) End-Users need to be *"cybersecurity aware"* in order to "drive safely in cyberspace"
3) *Operational Policies* are required with regards to the transportation of portable storage
4) *Training:* Every Enterprise & Government Agency should receive regular security training
5) *CSO:* Dedicated professional personnel such as a business *CSO/CISO* should be recruited to set the security policies and manage the training, upgrades, audit and compliance
6) *Engineering to International Cybersecurity Standards* is essential in order that the Information, Data and ICT Assets are uniformly secured against cyberattacks
7) *Apps:* Every month, cybercriminals create new means of attacking & penetrating previously secure systems, particularly the latest smart mobile devices and *end-user "apps*"…
8) *Policies:* There is greater need for rigorously enforced security policies for wireless networks since they are inherently more open to attack when used by "non-security" aware users

*Workshop Session 2 *

"Integrated Cyber-Technological Solutions for the 21stC Web2.0 World"

1 – The 21stC Cyber World	2 – ITU Global CyberAgenda	3 – Cyber Technical Solutions:A
4 – Cyber Technical Solutions:B	5–Physical Security Solutions:A	6–Physical Security Solutions:B
7 – "Cyber to Physical Attacks"	8 – "Physical to Cyber Attacks"	9–Integrated Security Benefits

ITU Global Cybersecurity Agenda (GCA) and other Useful Cybersecurity Programmes

- The ITU GCA is used as the primary framework in this workshop with its extensive archive of strategic frameworks, operational procedures & technical standards
- Technical Measures: Various other National and International Agencies have also evolved and implemented cybersecurity programmes that are of relevant and useful in the determination of technical solutions & operational measures:
  - *EU/ENISA:* Pan-European Cybersecurity Programme including the CERT Network, Identity Management and active work on the Implementation of the CoE Convention on Cybercrime
  - *USA/NIST:* National Institute of Standards and Technology with its "800 Series" of Special Publications from the Computer Security Division that focus upon all aspects of cybersecurity
  - *USA/ASIS:* American Society for Industrial Security which includes many publications such as guidelines for Business continuity & Disaster Recovery and Job Profile for the Role of CSO
  - *USA/CMU-CERT:* Carnegie Mellon University pioneered the concept of the CERT, and now manage the CERT Co-ordination Resource and Training Centre & a global partnership network
  - *UK/ISF:* Information Security Forum that is probably best known for its publication of the "Good Practice Guidelines for Information Security" that is available for free on-line download
  - *UK/Jericho Forum*: International ICT Forum focusing mainly upon the cybersecurity challenges of security the 21stC world of Web2.0 applications and mobile wireless devices
  - *ISO:* International Standards Organisation has defined and published the evolving 27000 Series of Security which includes "ISMS requirements", "Codes of Practice" & "Risk Management"

……Next we drill down into the spectrum of practical cybersecurity solutions against cybercrime

*Workshop Session 2 *

"Integrated Cyber-Technological Solutions for the 21stC Web2.0 World"

1 – The 21stC Cyber World	2 – ITU Global CyberAgenda	3 – Cyber Technical Solutions:A
4 – Cyber Technical Solutions:B	5–Physical Security Solutions:A	6–Physical Security Solutions:B
7 – "Cyber to Physical Attacks"	8 – "Physical to Cyber Attacks"	9–Integrated Security Benefits

Cyber Technical Solutions (A)

- Today we consider the real-world technical response to the most common forms of cybercrimes, cyberattacks and cyberterrorism:

1) Distributed Denial of Service
2) SQL Database Injection Attacks
3) XSS Cross-Site Scripting
4) Firewall Port Scanning
5) Malware, Spyware, Viruses, Worms and Trojans
6) Spam eMail and Phishing Scams
7) Keyloggers: Hardware and Software Variants
8) Transaction Security
9) Device and End-User Authentication
10) Cryptography: PKI and VPNs

….Jamaican Government and Enterprise ICT Facilities will all require professionally trained staff that are able to implement, manage and regularly upgrade cyber solutions…

ITU Cybersecurity Guide for Developing Countries

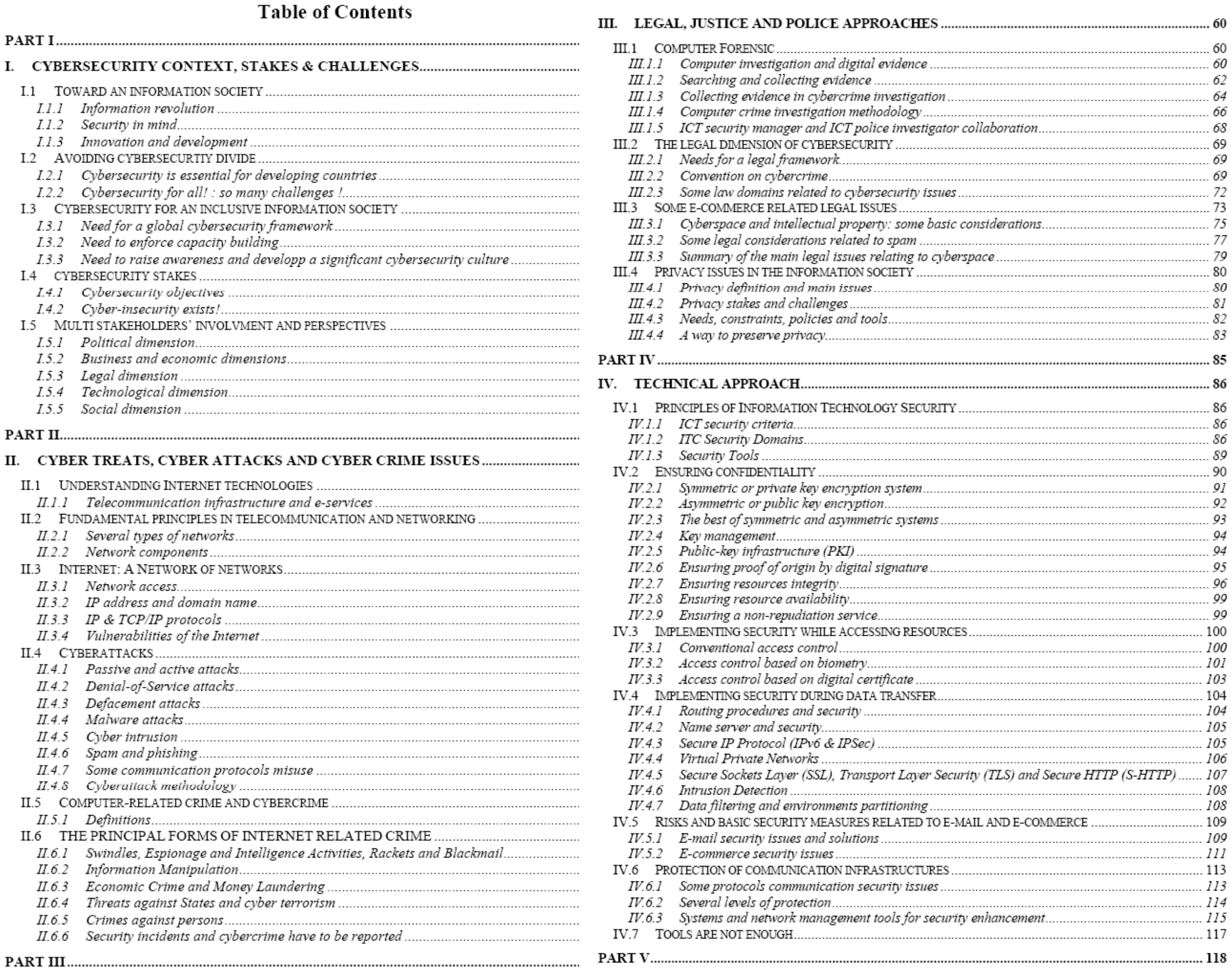


Table of Contents

PART I

I. CYBERSECURITY CONTEXT, STAKES & CHALLENGES

I.1 TOWARD AN INFORMATION SOCIETY
I.1.1 Information revolution
I.1.2 Security in mind
I.1.3 Innovation and development
I.2 AVOIDING CYBERSECURTIY DIVIDE
I.2.1 Cybersecurity is essential for developing countries
I.2.2 Cybersecurity for all! : so many challenges !
I.3 CYBERSECURITY FOR AN INCLUSIVE INFORMATION SOCIETY
I.3.1 Need for a global cybersecurity framework
I.3.2 Need to enforce capacity building
I.3.3 Need to raise awareness and developp a significant cybersecurity culture
I.4 CYBERSECURITY STAKES
I.4.1 Cybersecurity objectives
I.4.2 Cyber-insecurity exists!
I.5 MULTI STAKEHOLDERS' INVOLVMENT AND PERSPECTIVES
I.5.1 Political dimension
I.5.2 Business and economic dimensions
I.5.3 Legal dimension
I.5.4 Technological dimension
I.5.5 Social dimension

PART II

II. CYBER TREATS, CYBER ATTACKS AND CYBER CRIME ISSUES

II.1 UNDERSTANDING INTERNET TECHNOLOGIES
II.1.1 Telecommunication infrastructure and e-services
II.2 FUNDAMENTAL PRINCIPLES IN TELECOMMUNICATION AND NETWORKING
II.2.1 Several types of networks
II.2.2 Network components
II.3 INTERNET: A NETWORK OF NETWORKS
II.3.1 Network access
II.3.2 IP address and domain name
II.3.3 IP & TCP/IP protocols
II.3.4 Vulnerabilities of the Internet
II.4 CYBERATTACKS
II.4.1 Passive and active attacks
II.4.2 Denial-of-Service attacks
II.4.3 Defacement attacks
II.4.4 Malware attacks
II.4.5 Cyber intrusion
II.4.6 Spam and phishing
II.4.7 Some communication protocols misuse
II.4.8 Cyberattack methodology
II.5 COMPUTER-RELATED CRIME AND CYBERCRIME
II.5.1 Definitions
II.6 THE PRINCIPAL FORMS OF INTERNET RELATED CRIME
II.6.1 Swindles, Espionage and Intelligence Activities, Rackets and Blackmail
II.6.2 Information Manipulation
II.6.3 Economic Crime and Money Laundering
II.6.4 Threats against States and cyber terrorism
II.6.5 Crimes against persons
II.6.6 Security incidents and cybercrime have to be reported

PART III

III. LEGAL, JUSTICE AND POLICE APPROACHES ... 60

III.1 COMPUTER FORENSIC ... 60
III.1.1 Computer investigation and digital evidence ... 60
III.1.2 Searching and collecting evidence ... 62
III.1.3 Collecting evidence in cybercrime investigation ... 64
III.1.4 Computer crime investigation methodology ... 66
III.1.5 ICT security manager and ICT police investigator collaboration ... 68
III.2 THE LEGAL DIMENSION OF CYBERSECURITY ... 69
III.2.1 Needs for a legal framework ... 69
III.2.2 Convention on cybercrime ... 69
III.2.3 Some law domains related to cybersecurity issues ... 72
III.3 SOME E-COMMERCE RELATED LEGAL ISSUES ... 73
III.3.1 Cyberspace and intellectual property: some basic considerations ... 75
III.3.2 Some legal considerations related to spam ... 77
III.3.3 Summary of the main legal issues relating to cyberspace ... 79
III.4 PRIVACY ISSUES IN THE INFORMATION SOCIETY ... 80
III.4.1 Privacy definition and main issues ... 80
III.4.2 Privacy stakes and challenges ... 81
III.4.3 Needs, constraints, policies and tools ... 82
III.4.4 A way to preserve privacy ... 83

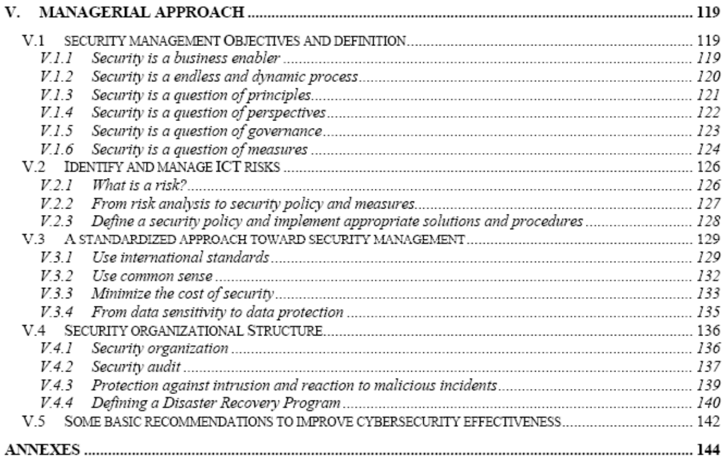
PART IV ... 85

IV. TECHNICAL APPROACH ... 86

IV.1 PRINCIPLES OF INFORMATION TECHNOLOGY SECURITY ... 86
IV.1.1 ICT security criteria ... 86
IV.1.2 ITC Security Domains ... 86
IV.1.3 Security Tools ... 89
IV.2 ENSURING CONFIDENTIALITY ... 90
IV.2.1 Symmetric or private key encryption system ... 91
IV.2.2 Asymmetric or public key encryption ... 92
IV.2.3 The best of symmetric and asymmetric systems ... 93
IV.2.4 Key management ... 94
IV.2.5 Public-key infrastructure (PKI) ... 94
IV.2.6 Ensuring proof of origin by digital signature ... 95
IV.2.7 Ensuring resources integrity ... 96
IV.2.8 Ensuring resource availability ... 99
IV.2.9 Ensuring a non-repudiation service ... 99
IV.3 IMPLEMENTING SECURITY WHILE ACCESSING RESOURCES ... 100
IV.3.1 Conventional access control ... 100
IV.3.2 Access control based on biometry ... 101
IV.3.3 Access control based on digital certificate ... 103
IV.4 IMPLEMENTING SECURITY DURING DATA TRANSFER ... 104
IV.4.1 Routing procedures and security ... 104
IV.4.2 Name server and security ... 105
IV.4.3 Secure IP Protocol (IPv6 & IPSec) ... 105
IV.4.4 Virtual Private Networks ... 106
IV.4.5 Secure Sockets Layer (SSL), Transport Layer Security (TLS) and Secure HTTP (S-HTTP) ... 107
IV.4.6 Intrusion Detection ... 108
IV.4.7 Data filtering and environments partitioning ... 108
IV.5 RISKS AND BASIC SECURITY MEASURES RELATED TO E-MAIL AND E-COMMERCE ... 109
IV.5.1 E-mail security issues and solutions ... 109
IV.5.2 E-commerce security issues ... 111
IV.6 PROTECTION OF COMMUNICATION INFRASTRUCTURES ... 113
IV.6.1 Some protocols communication security issues ... 113
IV.6.2 Several levels of protection ... 114
IV.6.3 Systems and network management tools for security enhancement ... 115
IV.7 TOOLS ARE NOT ENOUGH ... 117

PART V ... 118

Cybersecurity Guide for Developing Countries



V. MANAGERIAL APPROACH ... 119

V.1 SECURITY MANAGEMENT OBJECTIVES AND DEFINITION ... 119
V.1.1 Security is a business enabler ... 119
V.1.2 Security is a endless and dynamic process ... 120
V.1.3 Security is a question of principles ... 121
V.1.4 Security is a question of perspectives ... 122
V.1.5 Security is a question of governance ... 123
V.1.6 Security is a question of measures ... 124
V.2 IDENTIFY AND MANAGE ICT RISKS ... 126
V.2.1 What is a risk? ... 126
V.2.2 From risk analysis to security policy and measures ... 127
V.2.3 Define a security policy and implement appropriate solutions and procedures ... 128
V.3 A STANDARDIZED APPROACH TOWARD SECURITY MANAGEMENT ... 129
V.3.1 Use international standards ... 129
V.3.2 Use common sense ... 132
V.3.3 Minimize the cost of security ... 133
V.3.4 From data sensitivity to data protection ... 135
V.4 SECURITY ORGANIZATIONAL STRUCTURE ... 136
V.4.1 Security organization ... 136
V.4.2 Security audit ... 137
V.4.3 Protection against intrusion and reaction to malicious incidents ... 139
V.4.4 Defining a Disaster Recovery Program ... 140
V.5 SOME BASIC RECOMMENDATIONS TO IMPROVE CYBERSECURITY EFFECTIVENESS ... 142

ANNEXES ... 144

Distributed Denial of Service CyberAttack

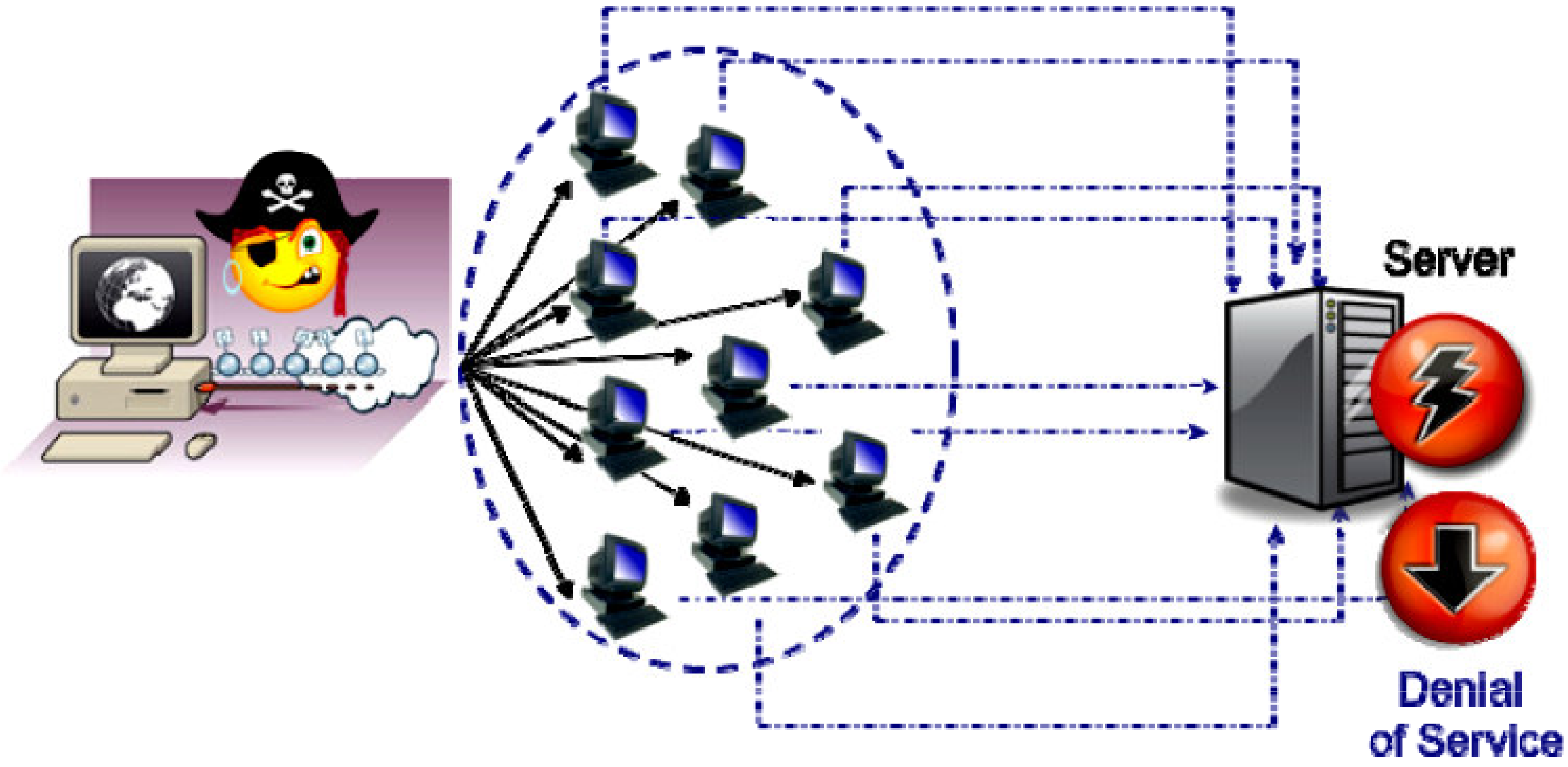
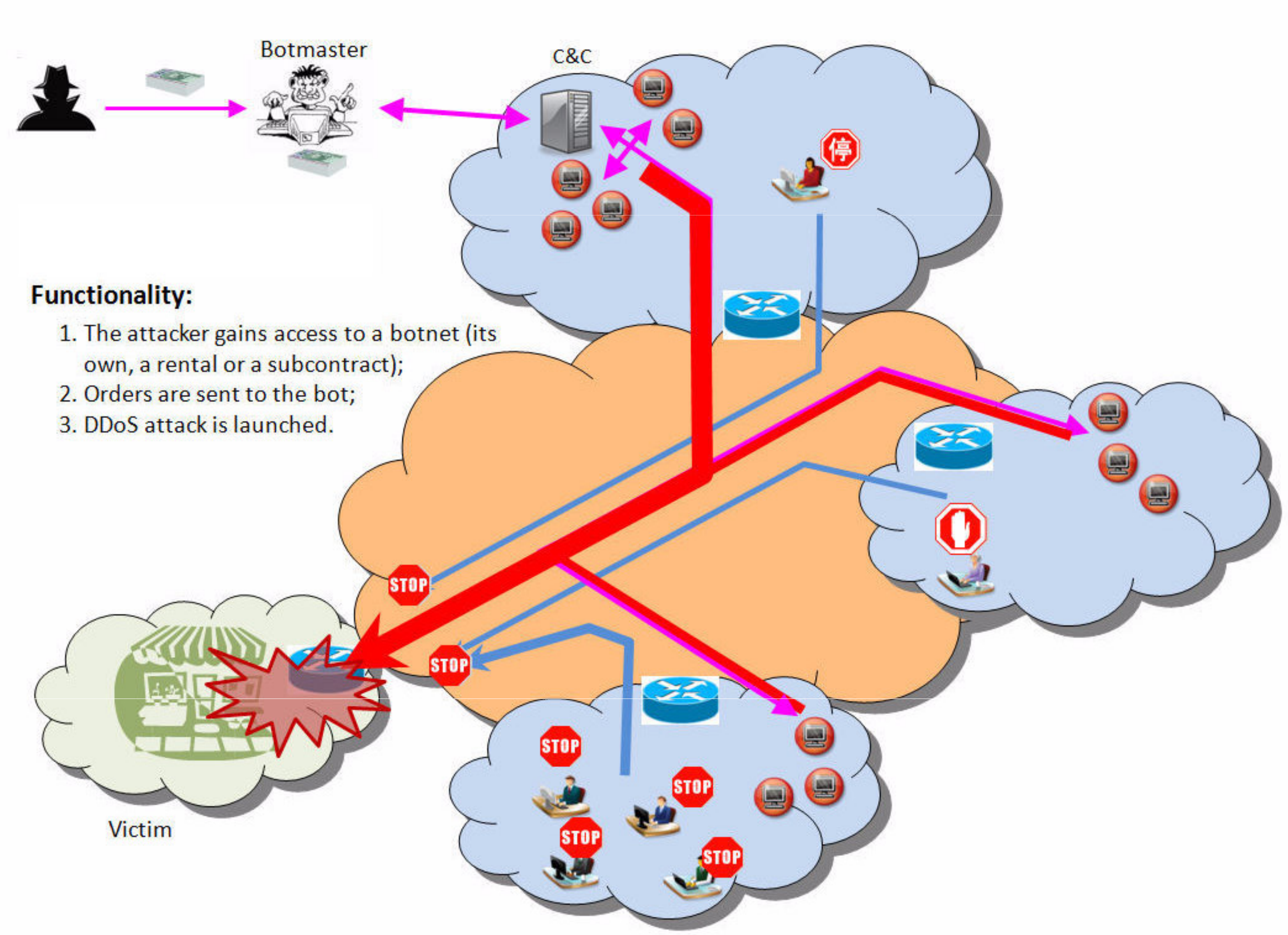


Figure II.7: Denial-of-service attack

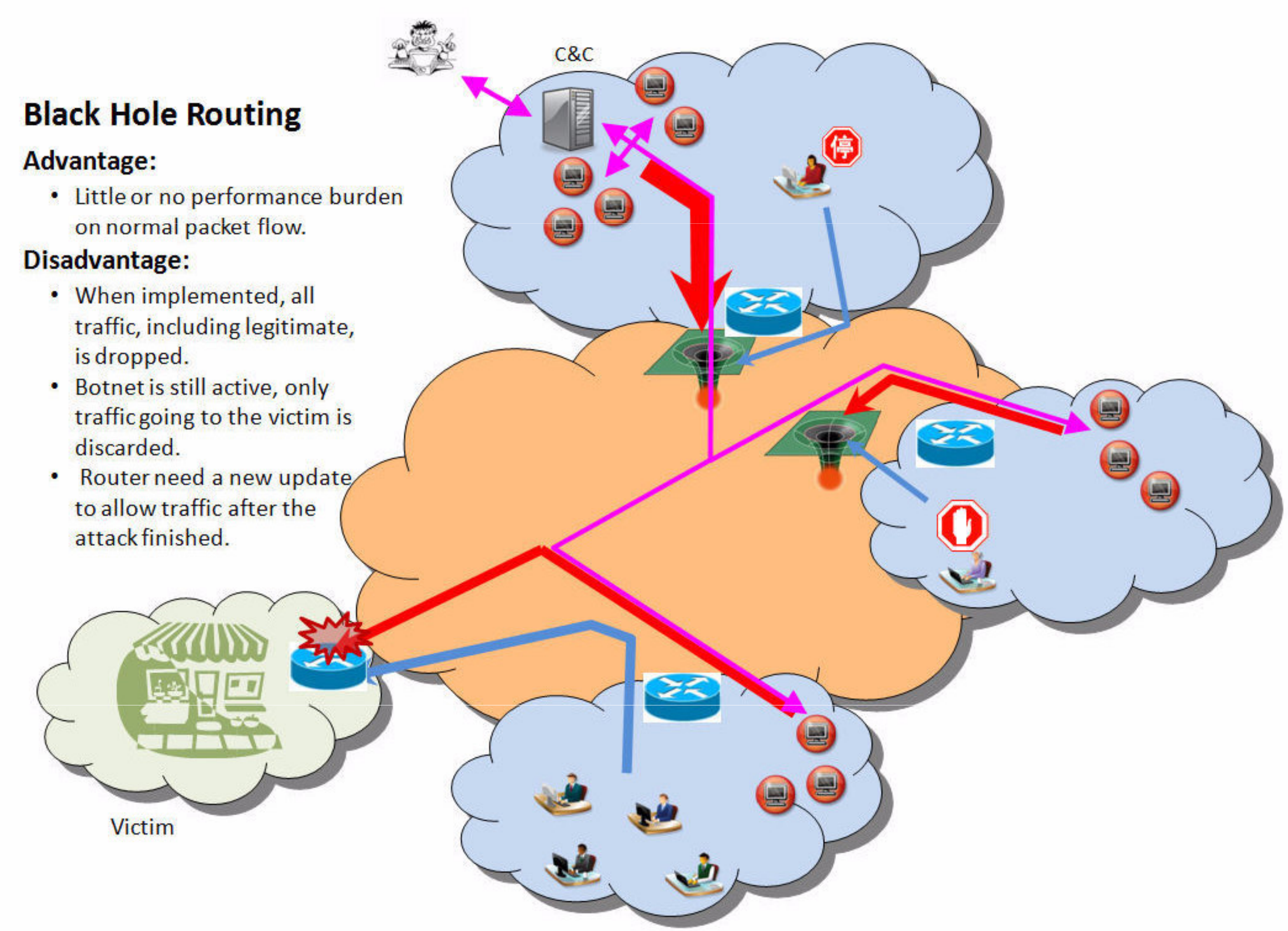
Typical DDOS BotNet Attack



Functionality:

1. The attacker gains access to a botnet (its own, a rental or a subcontract);
2. Orders are sent to the bot;
3. DDoS attack is launched.

Mitigate Attack: Black-Holing



Black Hole Routing

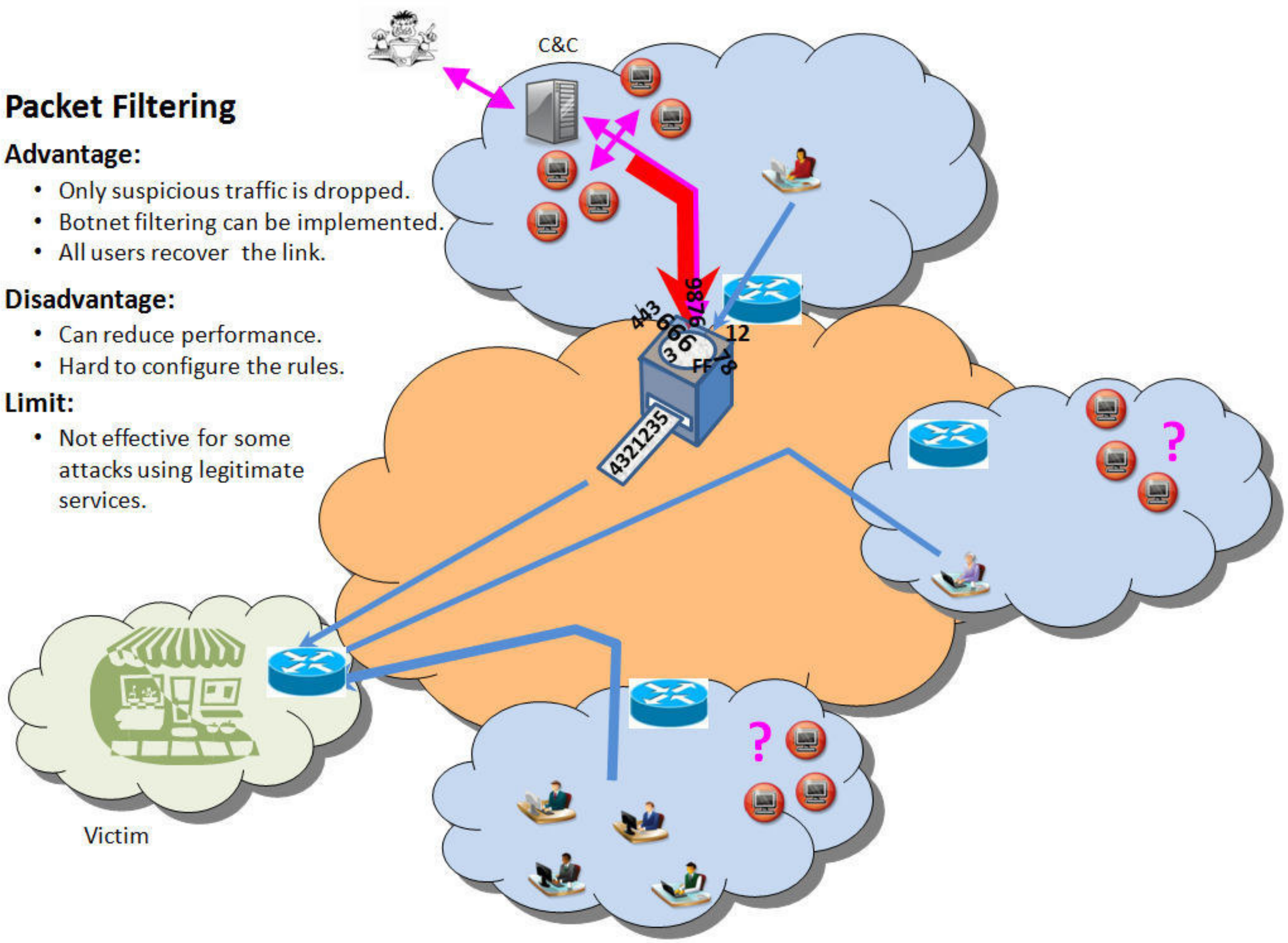
Advantage:

- Little or no performance burden on normal packet flow.

Disadvantage:

- When implemented, all traffic, including legitimate, is dropped.
- Botnet is still active, only traffic going to the victim is discarded.
- Router need a new update to allow traffic after the attack finished.

Mitigate Attack: Packet Filter



Packet Filtering

Advantage:

- Only suspicious traffic is dropped.
- Botnet filtering can be implemented.
- All users recover the link.

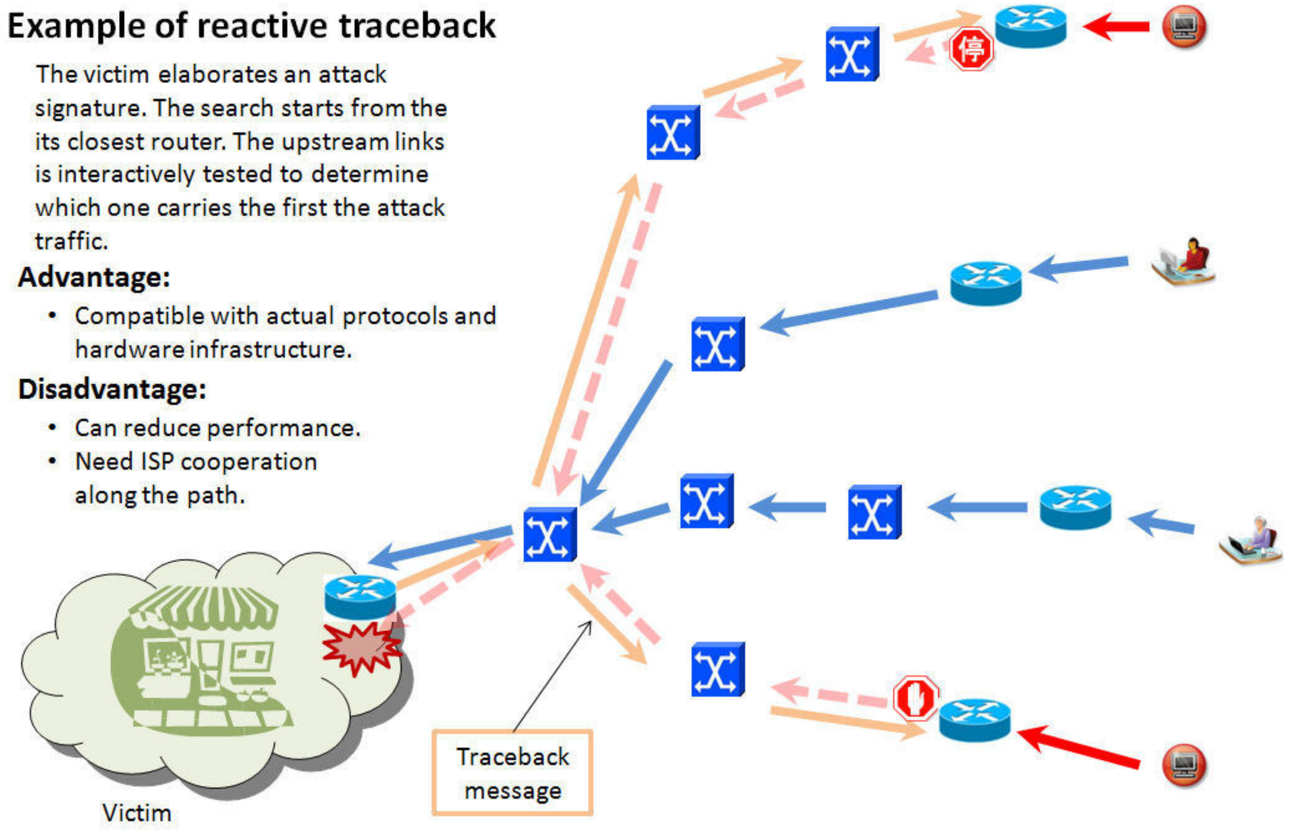
Disadvantage:

- Can reduce performance.
- Hard to configure the rules.

Limit:

- Not effective for some attacks using legitimate services.

DDOS Reactive Traceback



Example of reactive traceback

The victim elaborates an attack signature. The search starts from the its closest router. The upstream links is interactively tested to determine which one carries the first the attack traffic.

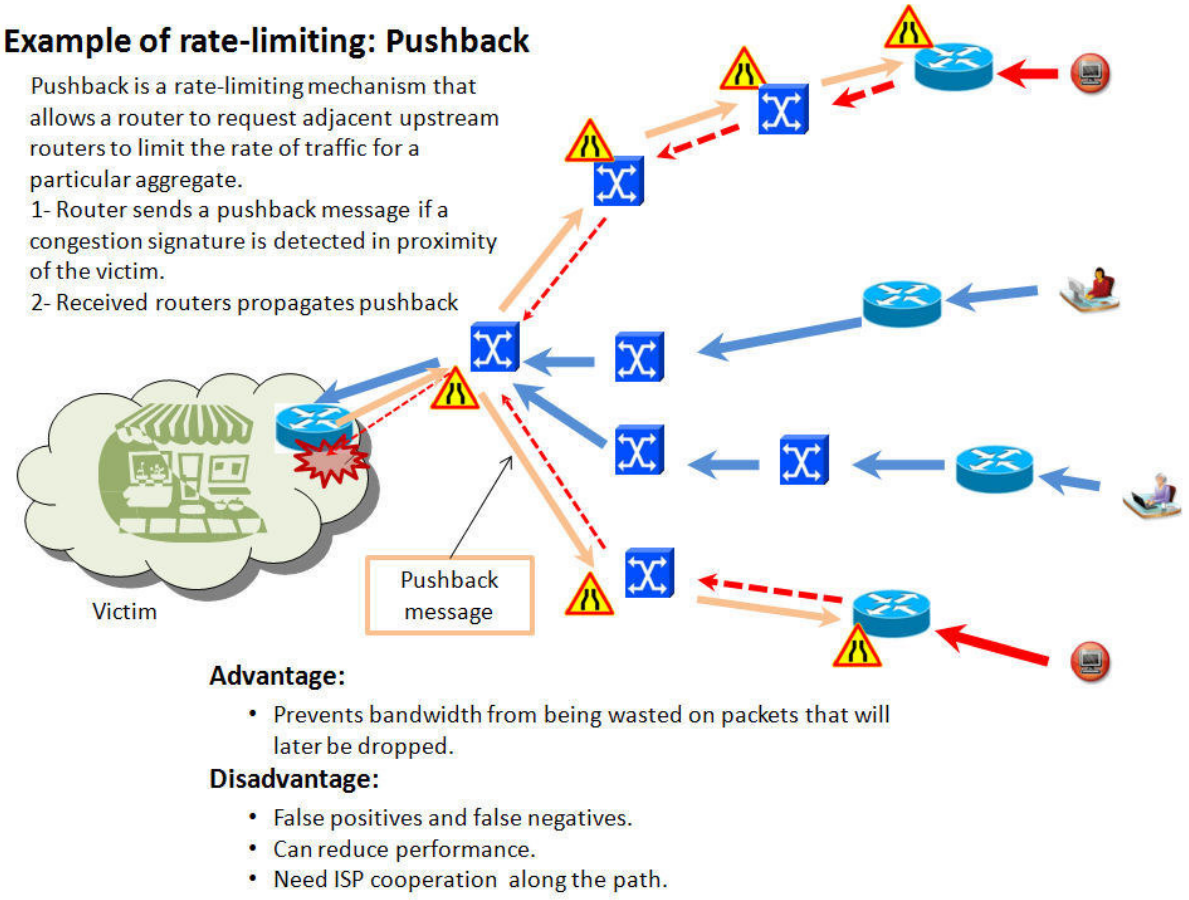
Advantage:

- Compatible with actual protocols and hardware infrastructure.

Disadvantage:

- Can reduce performance.
- Need ISP cooperation along the path.

DDOS Traffic Rate Limiting



Example of rate-limiting: Pushback

Pushback is a rate-limiting mechanism that allows a router to request adjacent upstream routers to limit the rate of traffic for a particular aggregate.

1- Router sends a pushback message if a congestion signature is detected in proximity of the victim.

2- Received routers propagates pushback

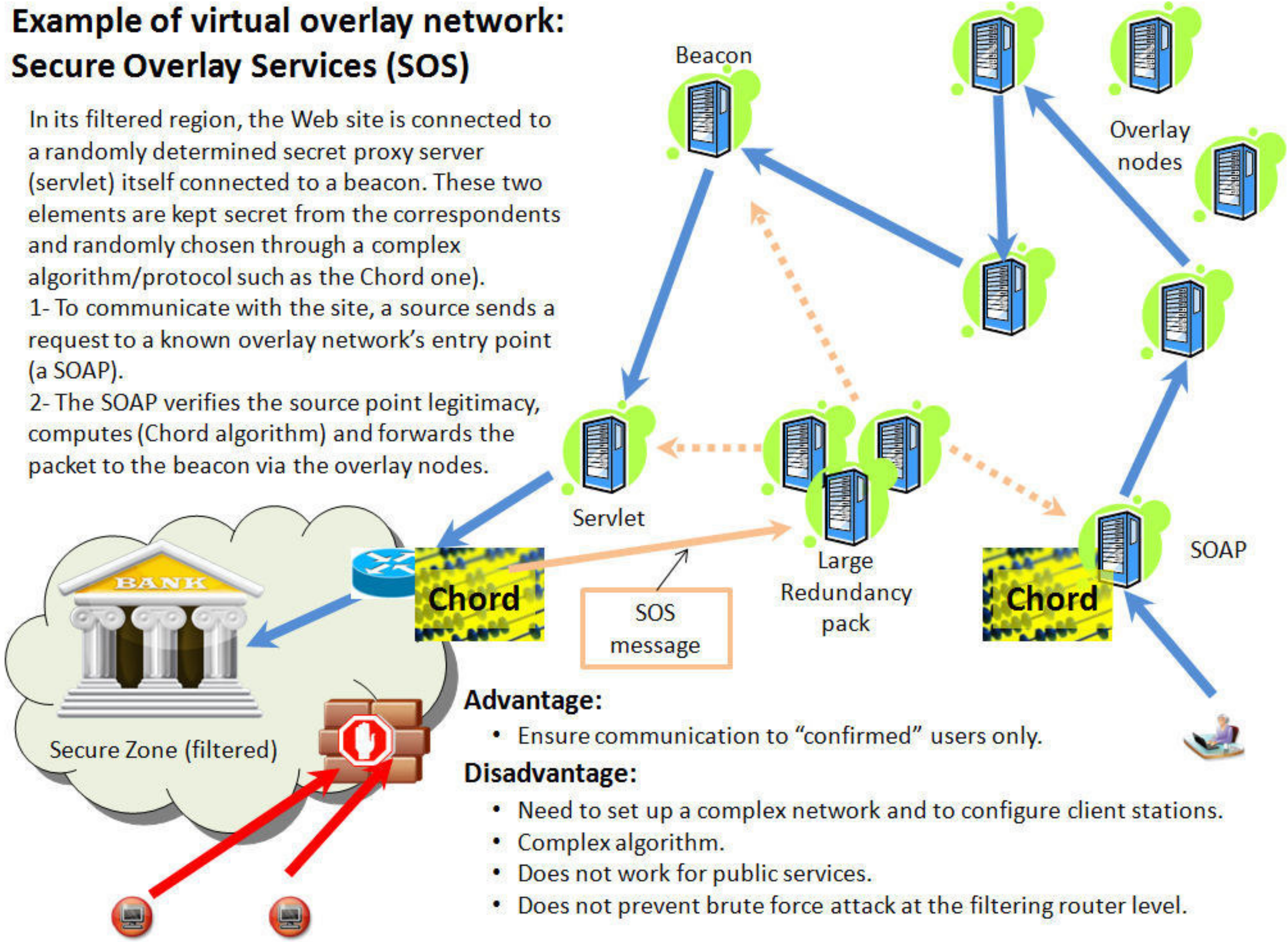
Advantage:

- Prevents bandwidth from being wasted on packets that will later be dropped.

Disadvantage:

- False positives and false negatives.
- Can reduce performance.
- Need ISP cooperation along the path.

DDOS: Virtual Overlay Network



Example of virtual overlay network: Secure Overlay Services (SOS)

In its filtered region, the Web site is connected to a randomly determined secret proxy server (servlet) itself connected to a beacon. These two elements are kept secret from the correspondents and randomly chosen through a complex algorithm/protocol such as the Chord one).

1- To communicate with the site, a source sends a request to a known overlay network's entry point (a SOAP).

2- The SOAP verifies the source point legitimacy, computes (Chord algorithm) and forwards the packet to the beacon via the overlay nodes.

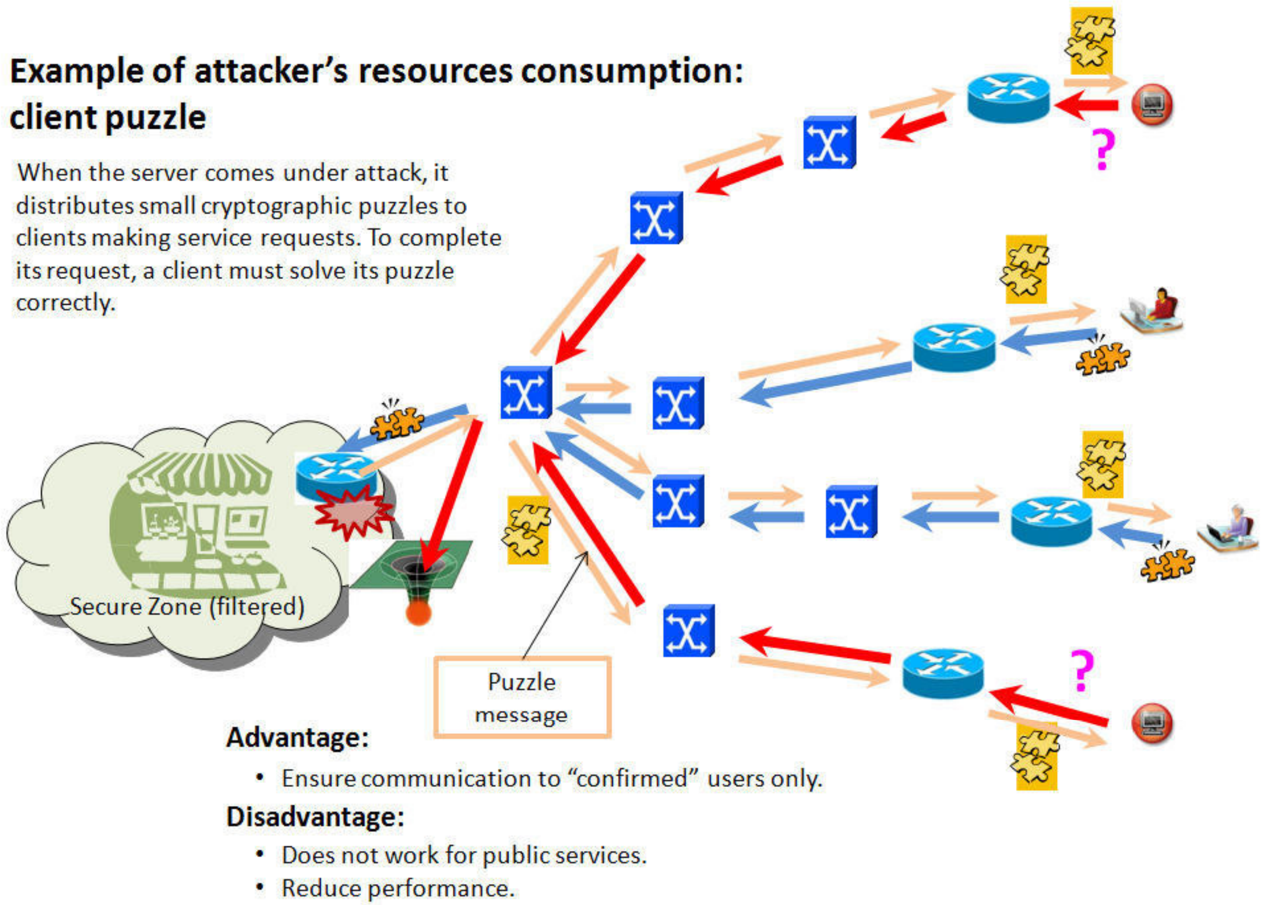
Advantage:

- Ensure communication to "confirmed" users only.

Disadvantage:

- Need to set up a complex network and to configure client stations.
- Complex algorithm.
- Does not work for public services.
- Does not prevent brute force attack at the filtering router level.

DDOS Mitigation: Cyptographic Puzzles



Example of attacker's resources consumption: client puzzle

When the server comes under attack, it distributes small cryptographic puzzles to clients making service requests. To complete its request, a client must solve its puzzle correctly.

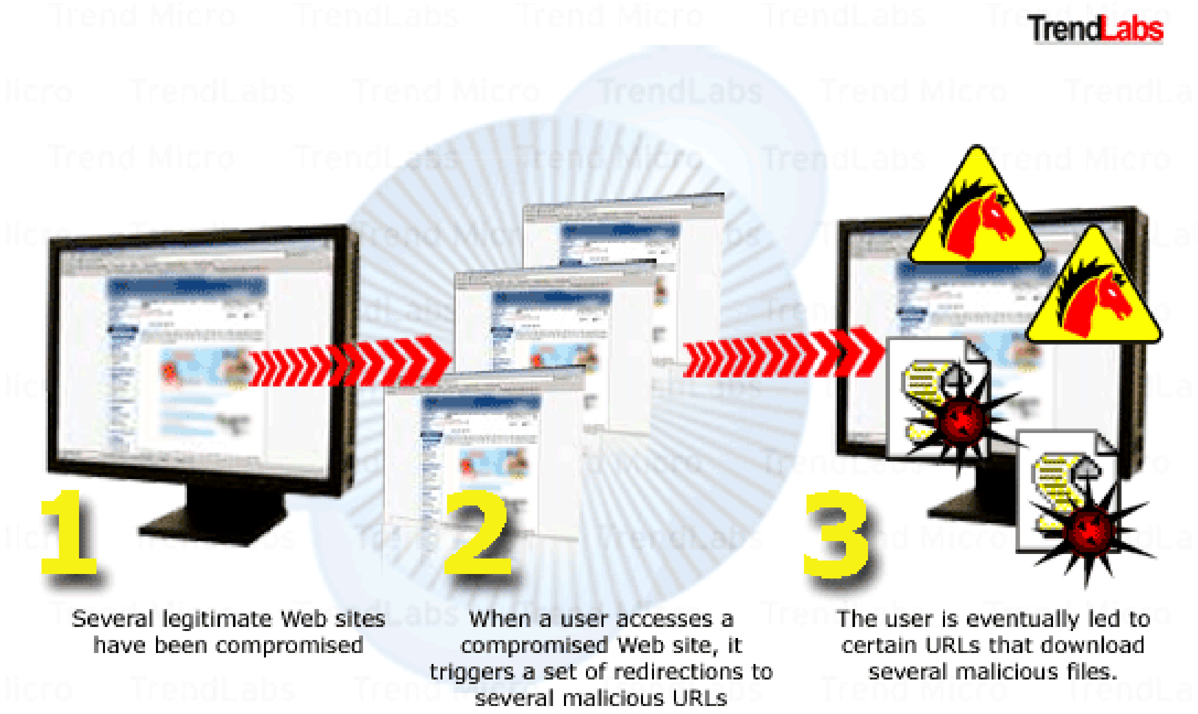
Advantage:

- Ensure communication to "confirmed" users only.

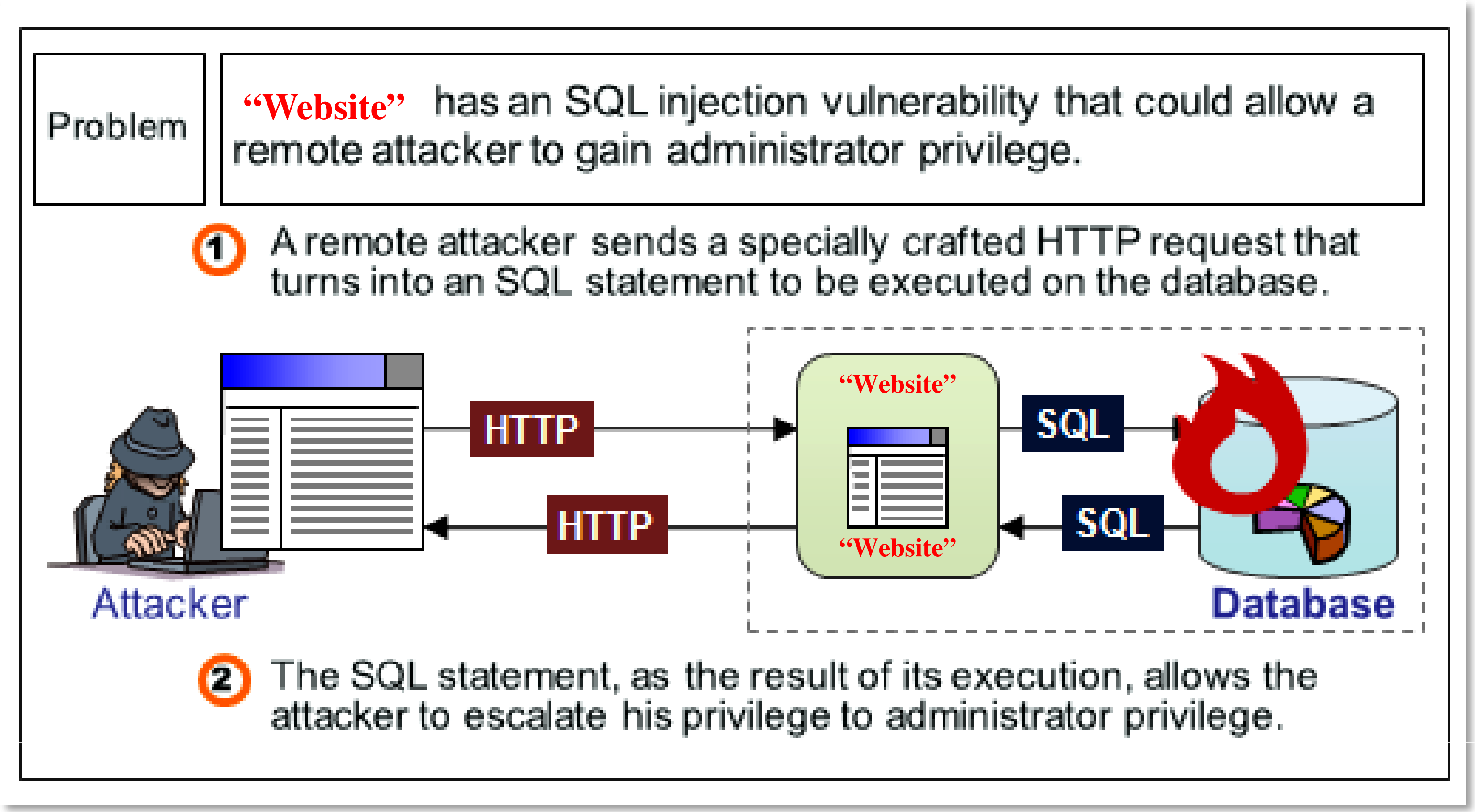
Disadvantage:

- Does not work for public services.
- Reduce performance.

SQL Database Injection Attacks


TrendLabs
1
Several legitimate Web sites have been compromised
2
When a user accesses a compromised Web site, it triggers a set of redirections to several malicious URLs
3
The user is eventually led to certain URLs that download several malicious files.

SQL Injection Vulnerability



Problem

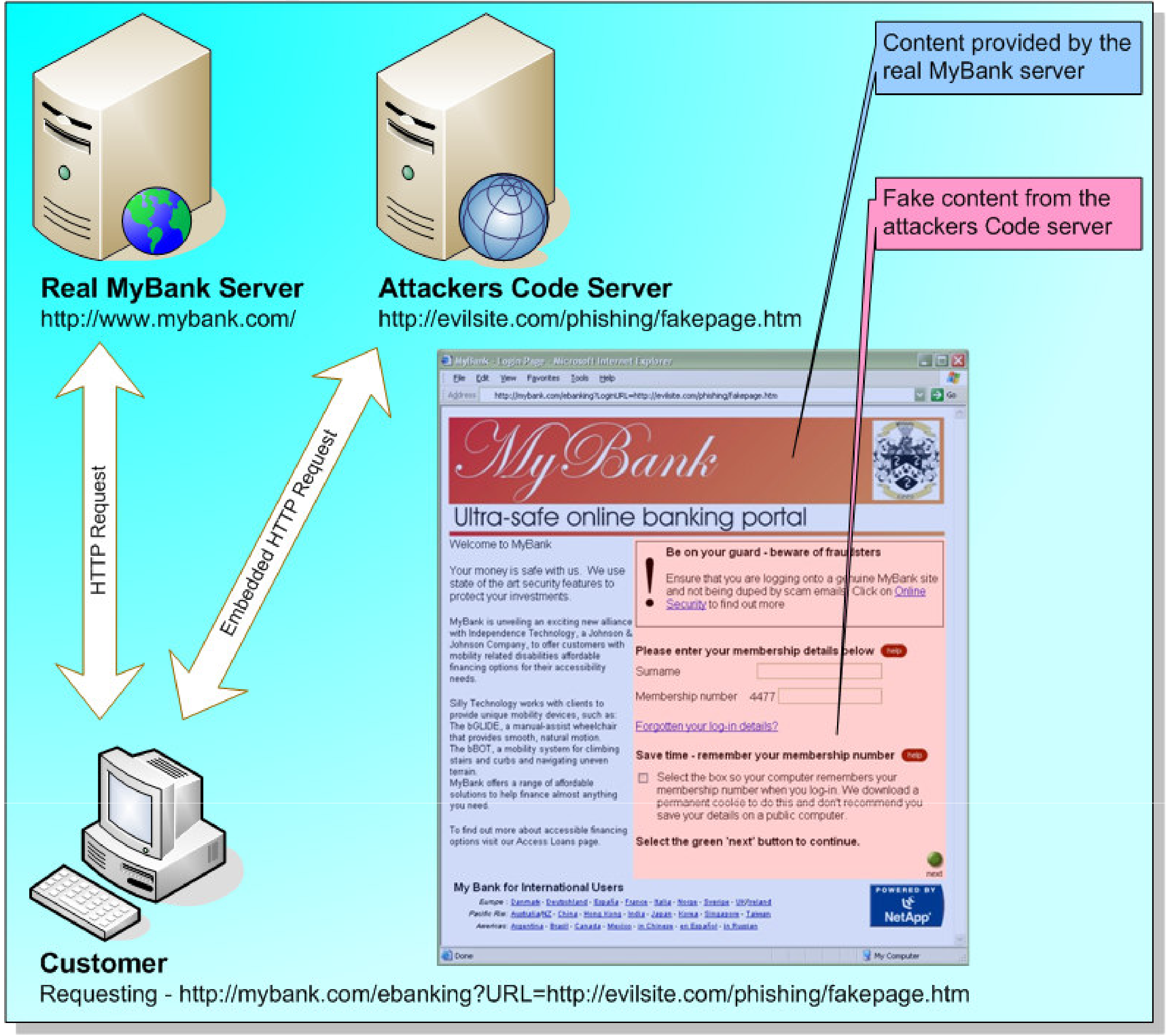
"Website" has an SQL injection vulnerability that could allow a remote attacker to gain administrator privilege.

1. A remote attacker sends a specially crafted HTTP request that turns into an SQL statement to be executed on the database.

2. The SQL statement, as the result of its execution, allows the attacker to escalate his privilege to administrator privilege.

Solution: Ensure all SQL user inputs are inserted into parameterised statements

Impact of XSS Cross-Site Scripting



Content provided by the real MyBank server
Fake content from the attackers Code server
Real MyBank Server
http://www.mybank.com/
Attackers Code Server
http://evilsite.com/phishing/fakepage.htm
HTTP Request
Embedded HTTP Request
Customer
Requesting - http://mybank.com/ebanking?URL=http://evilsite.com/phishing/fakepage.htm
MyBank - Login Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://mybank.com/ebanking?LoginURL=http://evilsite.com/phishing/fakepage.htm
Go
MyBank
Done
My Computer
POWERED BY NetApp

Ultra-safe online banking portal

Welcome to MyBank

Your money is safe with us. We use state of the art security features to protect your investments.

MyBank is unveiling an exciting new alliance with Independence Technology, a Johnson & Johnson Company, to offer customers with mobility related disabilities affordable financing options for their accessibility needs.

Silly Technology works with clients to provide unique mobility devices, such as: The bGLIDE, a manual-assist wheelchair that provides smooth, natural motion. The bBOT, a mobility system for climbing stairs and curbs and navigating uneven terrain. MyBank offers a range of affordable solutions to help finance almost anything you need.

To find out more about accessible financing options visit our Access Loans page.

Be on your guard - beware of fraudsters

! Ensure that you are logging onto a genuine MyBank site and not being duped by scam emails. Click on Online Security to find out more

Please enter your membership details below help

Surname

Membership number 4477

Forgotten your log-in details?

Save time - remember your membership number help

□ Select the box so your computer remembers your membership number when you log-in. We download a permanent cookie to do this and don't recommend you save your details on a public computer.

Select the green 'next' button to continue.

next

My Bank for International Users

Europe : Danmark - Deutschland - España - France - Italia - Norge - Sverige - UK/Ireland
Pacific Rim: Australia/NZ - China - Hong Kong - India - Japan - Korea - Singapore - Taiwan
Americas: Argentina - Brasil - Canada - Mexico - in Chinese - en Español - in Russian

Solution: Always check rigorously for data fields that allow user-input.

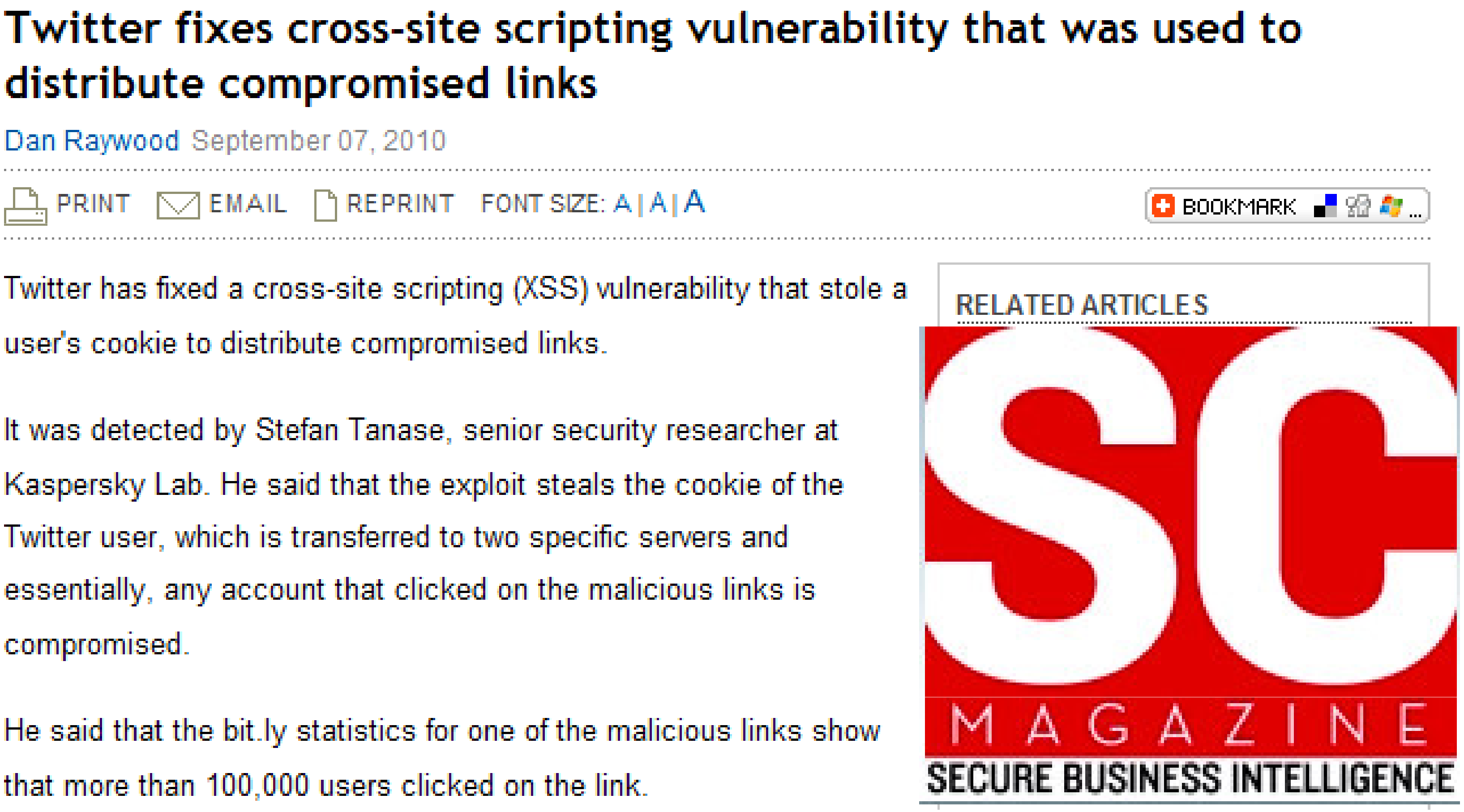
Ensure that there is no possibility for User Script input to be executed in website coded “php” or “asp” pages…

University of Technology, Jamaica

International Telecommunication Union

Committed to connecting the world

"Twitter" Cross-Site Scripting Vulnerability



Twitter fixes cross-site scripting vulnerability that was used to distribute compromised links

Dan Raywood September 07, 2010

Twitter has fixed a cross-site scripting (XSS) vulnerability that stole a user's cookie to distribute compromised links.

It was detected by Stefan Tanase, senior security researcher at Kaspersky Lab. He said that the exploit steals the cookie of the Twitter user, which is transferred to two specific servers and essentially, any account that clicked on the malicious links is compromised.

He said that the bit.ly statistics for one of the malicious links show that more than 100,000 users clicked on the link.

Functional Structure of a DMZ Firewall

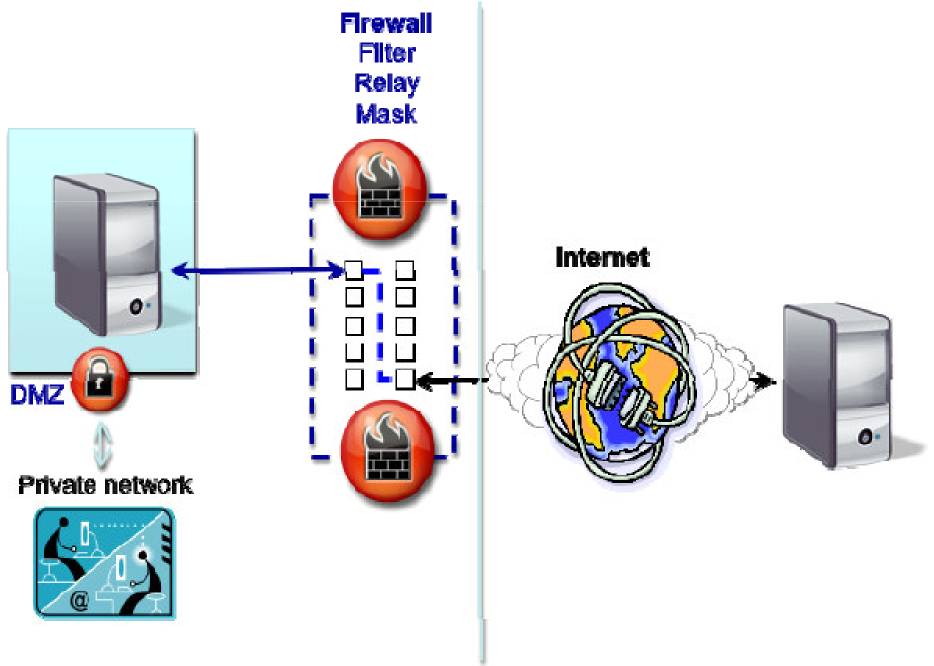
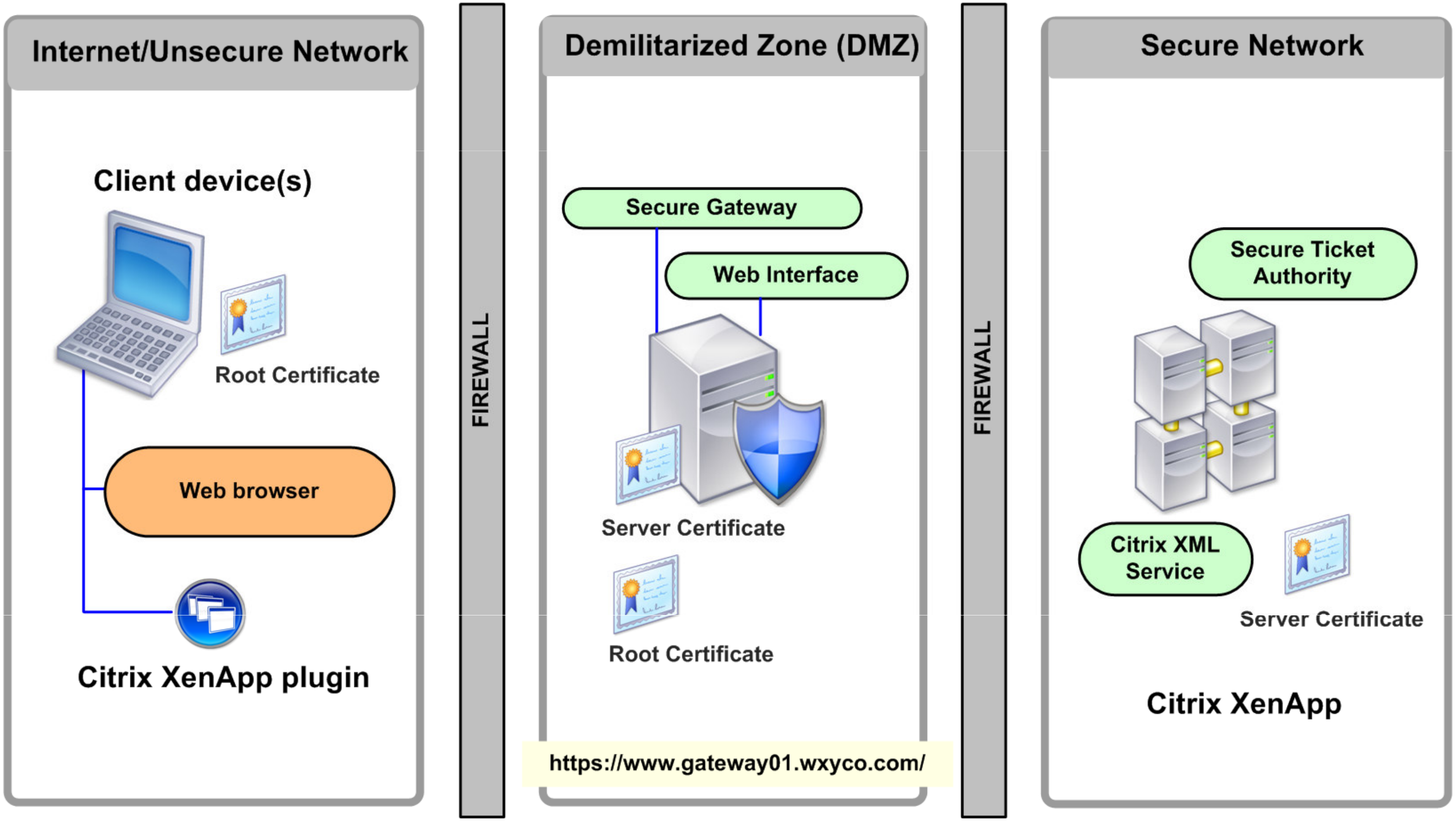


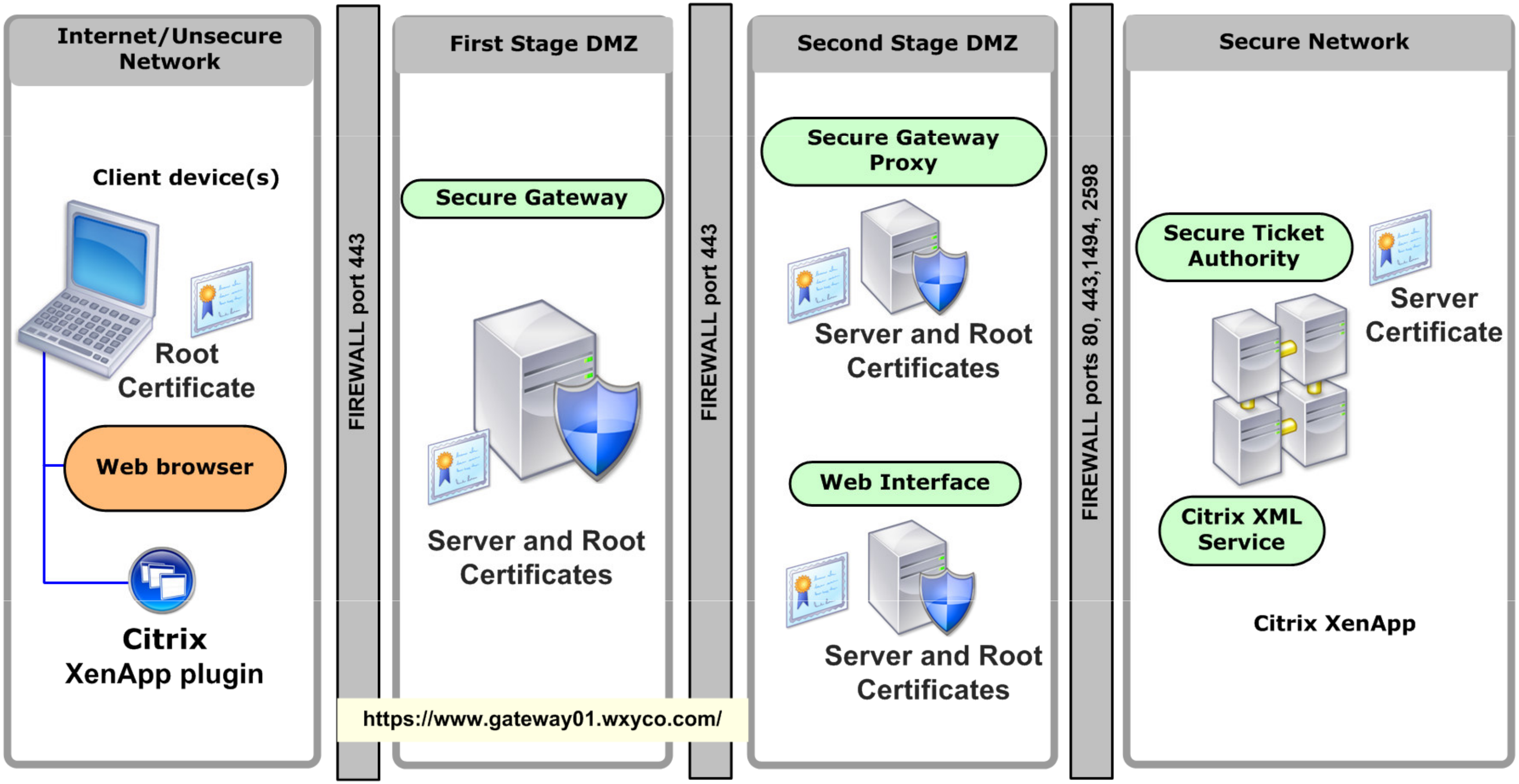
Figure IV.13: Functional structure of a firewall

Ensure that all firewall "ports" are locked down except those that are essential to operations,
And also implement dual firewalls with full DMZ (De-Militarised Zones) for further security

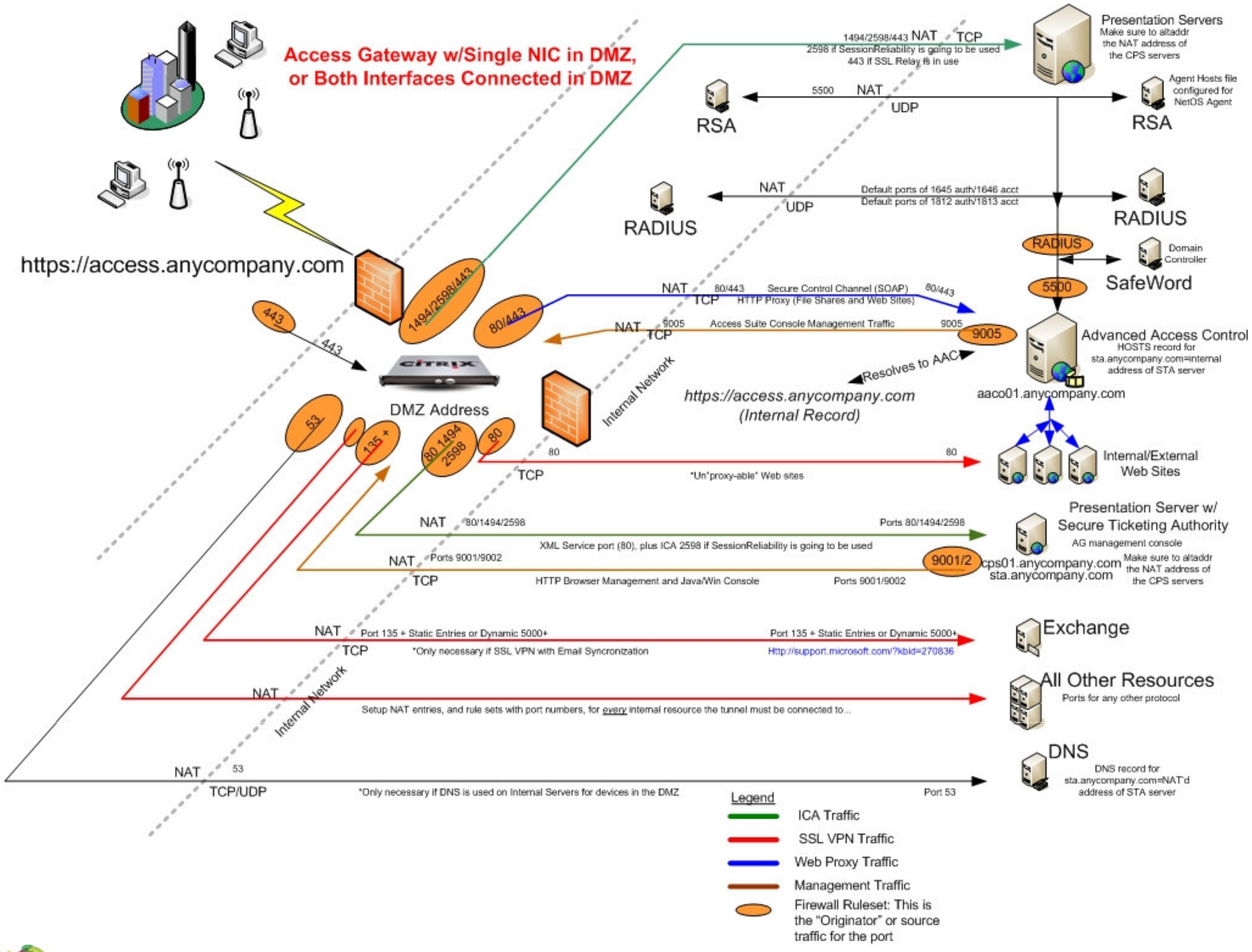
Typical Secure “Single-Hop” DMZ Firewall Configuration



Fully Secure "Double-Hop" DMZ Firewall Configuration



Single-Hop DMZ & Secure Network



Access Gateway w/Single NIC in DMZ, or Both Interfaces Connected in DMZ

https://access.anycompany.com

443

443

1494/2598/443

80/443

DMZ Address

53

135 +

80 1494 2598

80

Internal Network

Internal Network

1494/2598/443 NAT TCP
2598 if SessionReliability is going to be used
443 if SSL Relay is in use

Presentation Servers
Make sure to altaddr the NAT address of the CPS servers

5500 NAT UDP

RSA

Agent Hosts file configured for NetOS Agent

RSA

NAT UDP

Default ports of 1645 auth/1646 acct
Default ports of 1812 auth/1813 acct

RADIUS

RADIUS

RADIUS

Domain Controller

5500

SafeWord

NAT TCP 80/443 Secure Control Channel (SOAP) 80/443
HTTP Proxy (File Shares and Web Sites)

NAT TCP 9005 Access Suite Console Management Traffic 9005

9005

Advanced Access Control
HOSTS record for sta.anycompany.com=internal address of STA server

Resolves to AAC

https://access.anycompany.com
(Internal Record)

aaco01.anycompany.com

80 TCP 80
"Un"proxy-able" Web sites

Internal/External Web Sites

NAT 80/1494/2598 Ports 80/1494/2598
XML Service port (80), plus ICA 2598 if SessionReliability is going to be used

Presentation Server w/ Secure Ticketing Authority
AG management console

NAT Ports 9001/9002
TCP HTTP Browser Management and Java/Win Console Ports 9001/9002

9001/2

cps01.anycompany.com
sta.anycompany.com

Make sure to altaddr the NAT address of the CPS servers

NAT Port 135 + Static Entries or Dynamic 5000+ Port 135 + Static Entries or Dynamic 5000+
TCP *Only necessary if SSL VPN with Email Syncronization Http://support.microsoft.com/?kbid=270836

Exchange

NAT
Setup NAT entries, and rule sets with port numbers, for every internal resource the tunnel must be connected to...

All Other Resources
Ports for any other protocol

NAT 53
TCP/UDP *Only necessary if DNS is used on Internal Servers for devices in the DMZ Port 53

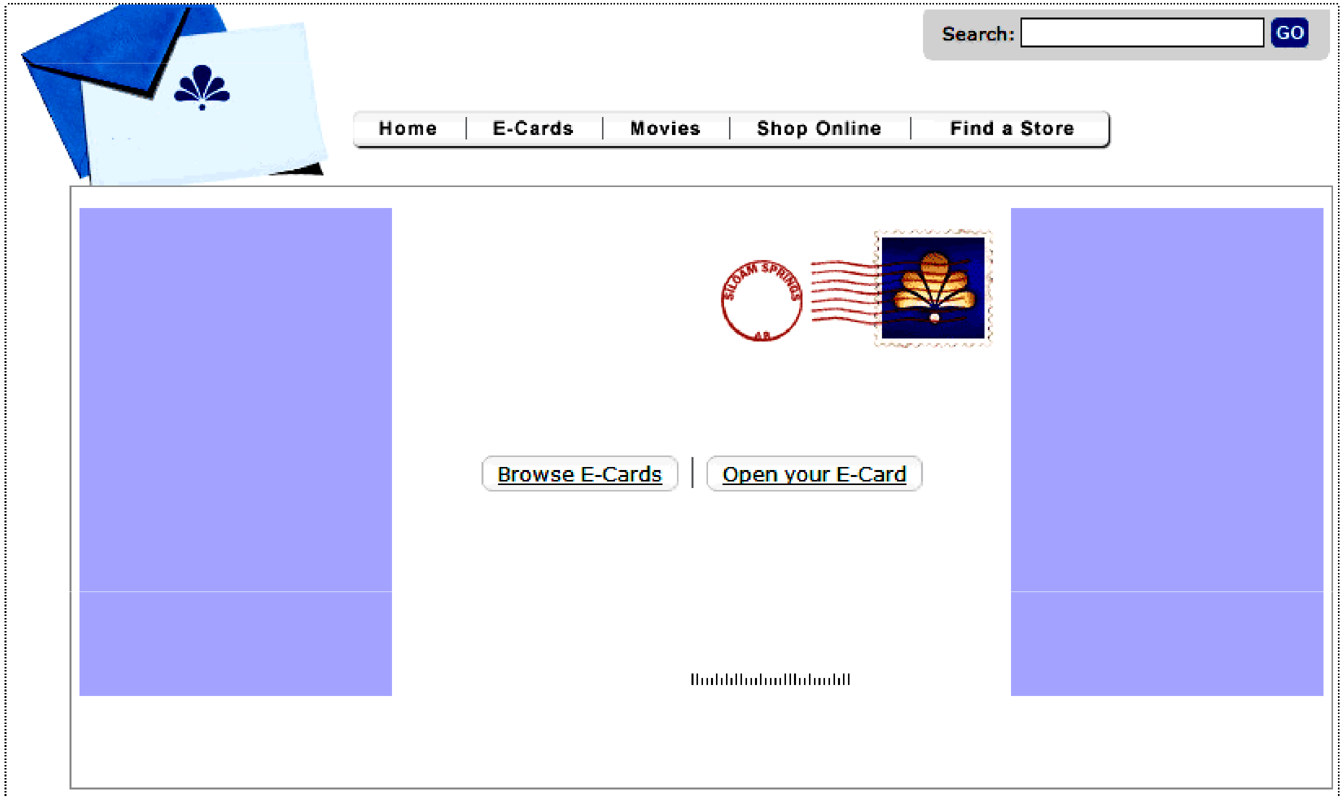
DNS
DNS record for sta.anycompany.com=NAT'd address of STA server

Legend

- 🟩 ICA Traffic
- 🟥 SSL VPN Traffic
- 🟦 Web Proxy Traffic
- 🟫 Management Traffic
- ● Firewall Ruleset: This is the "Originator" or source traffic for the port

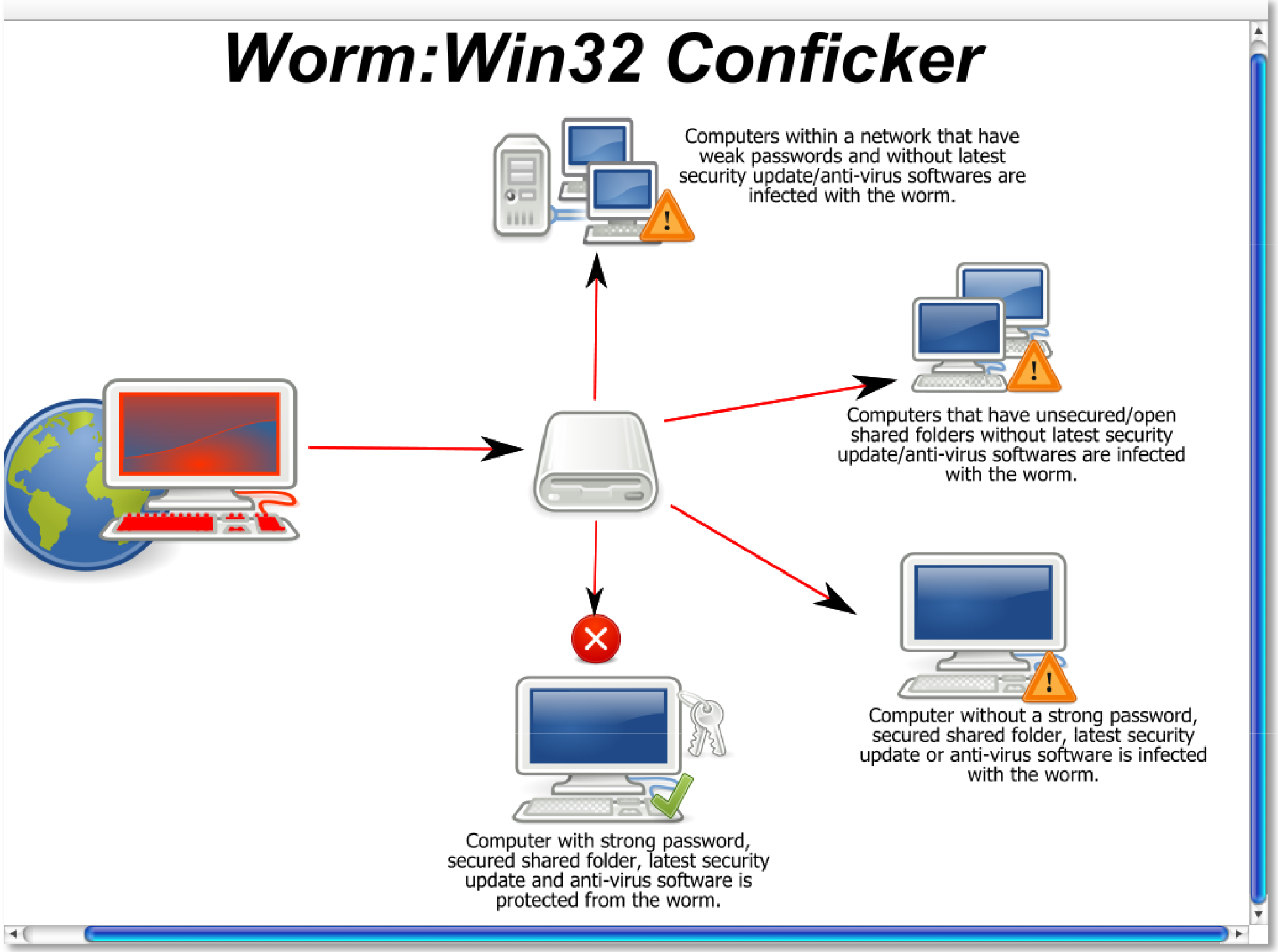
Malware, Spyware, Viruses, Worms & Trojans

- Trojans appear to users as attractive applications or messages such as the following generic eGreetings Card! Clicking on the card will then result in an "exe" file downloading malicious code to your PC, which may then open a permanent "back-door"



"Worm" Attacks: Defence requires fully implemented Cybersecurity Policies

Example: Win32 Conicker Worm – Self-Replicating – In-Built Self Defence – Infected more than 7Million Computers Worldwide since November 2008



Worm:Win32 Conficker
Computers within a network that have weak passwords and without latest security update/anti-virus softwares are infected with the worm.
Computers that have unsecured/open shared folders without latest security update/anti-virus softwares are infected with the worm.
Computer without a strong password, secured shared folder, latest security update or anti-virus software is infected with the worm.
Computer with strong password, secured shared folder, latest security update and anti-virus software is protected from the worm.

Spyware Attack

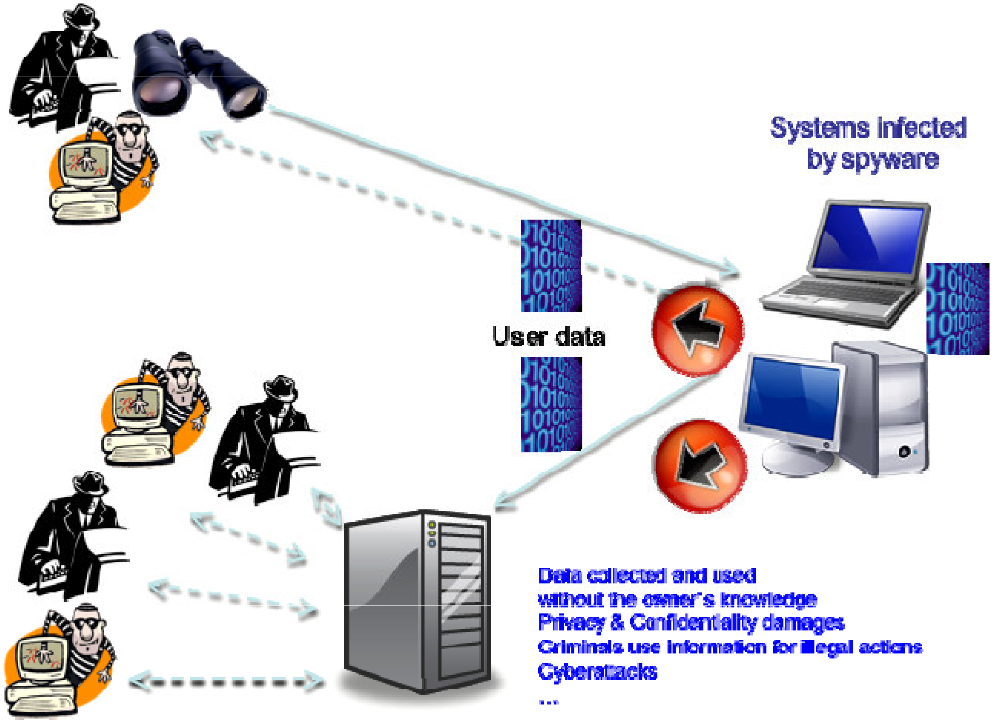
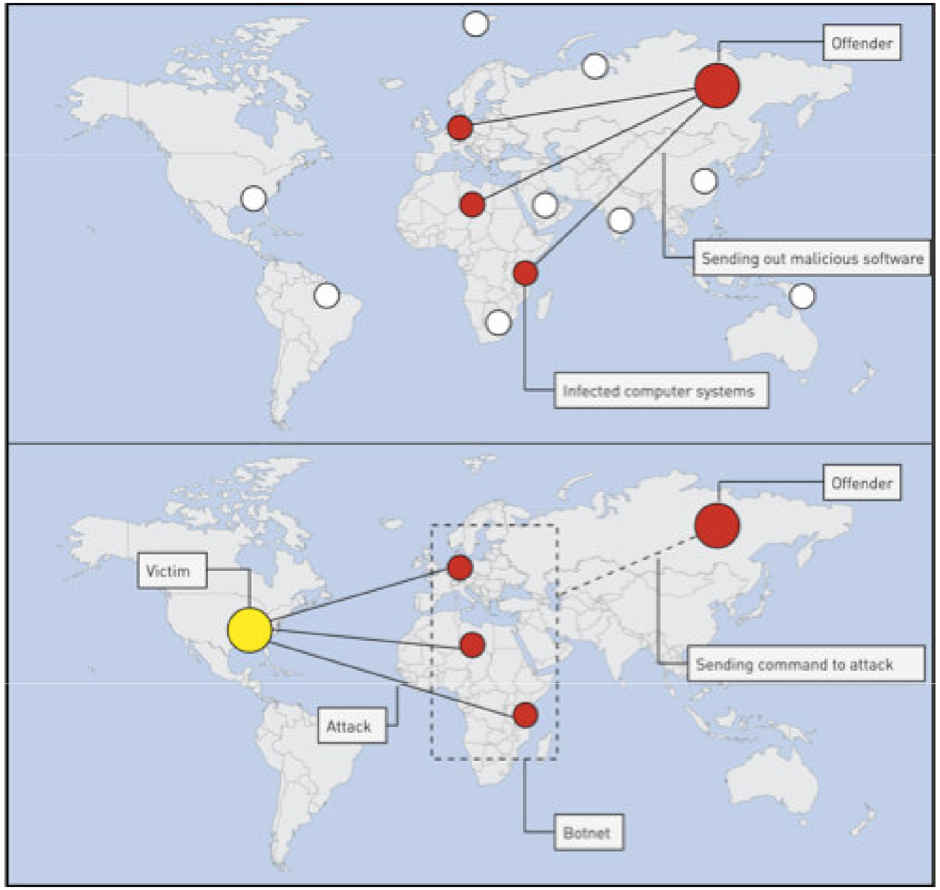

Systems infected by spyware
User data
Data collected and used without the owner's knowledge
Privacy & Confidentiality damages
Criminals use information for illegal actions
Cyberattacks
...

Figure II.8: Spyware attack

Global Spam Mail Attacks


Offender
Sending out malicious software
Infected computer systems
Offender
Victim
Sending command to attack
Attack
Botnet

Phishing Attack

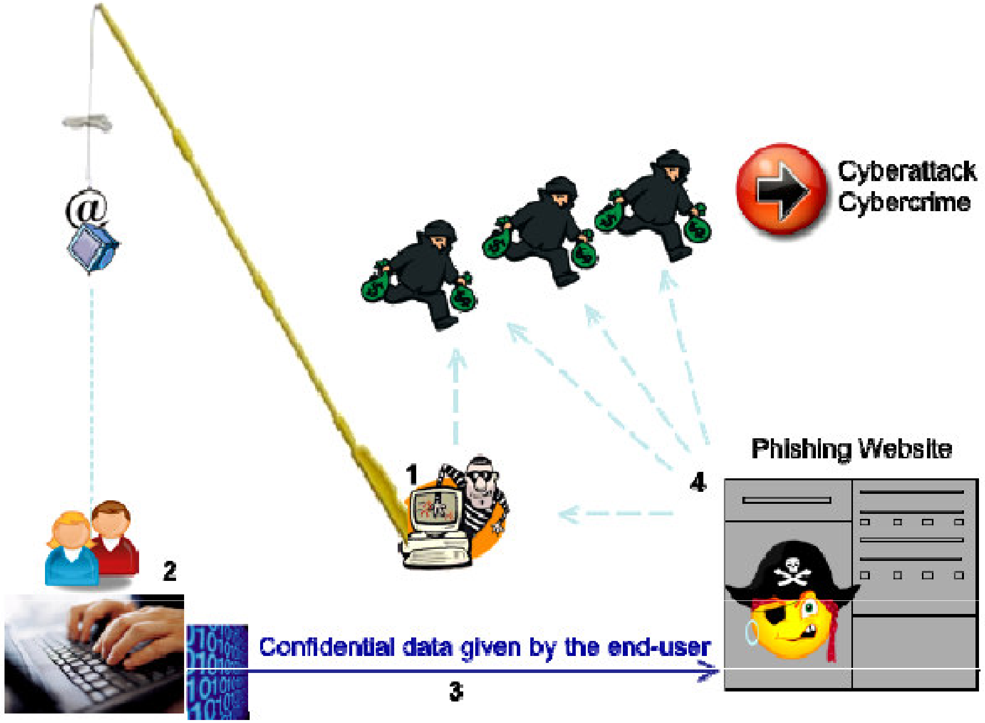
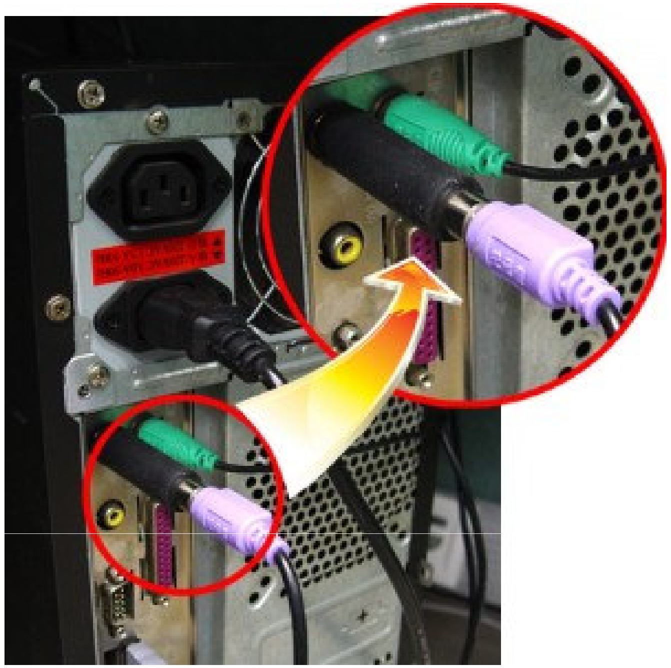


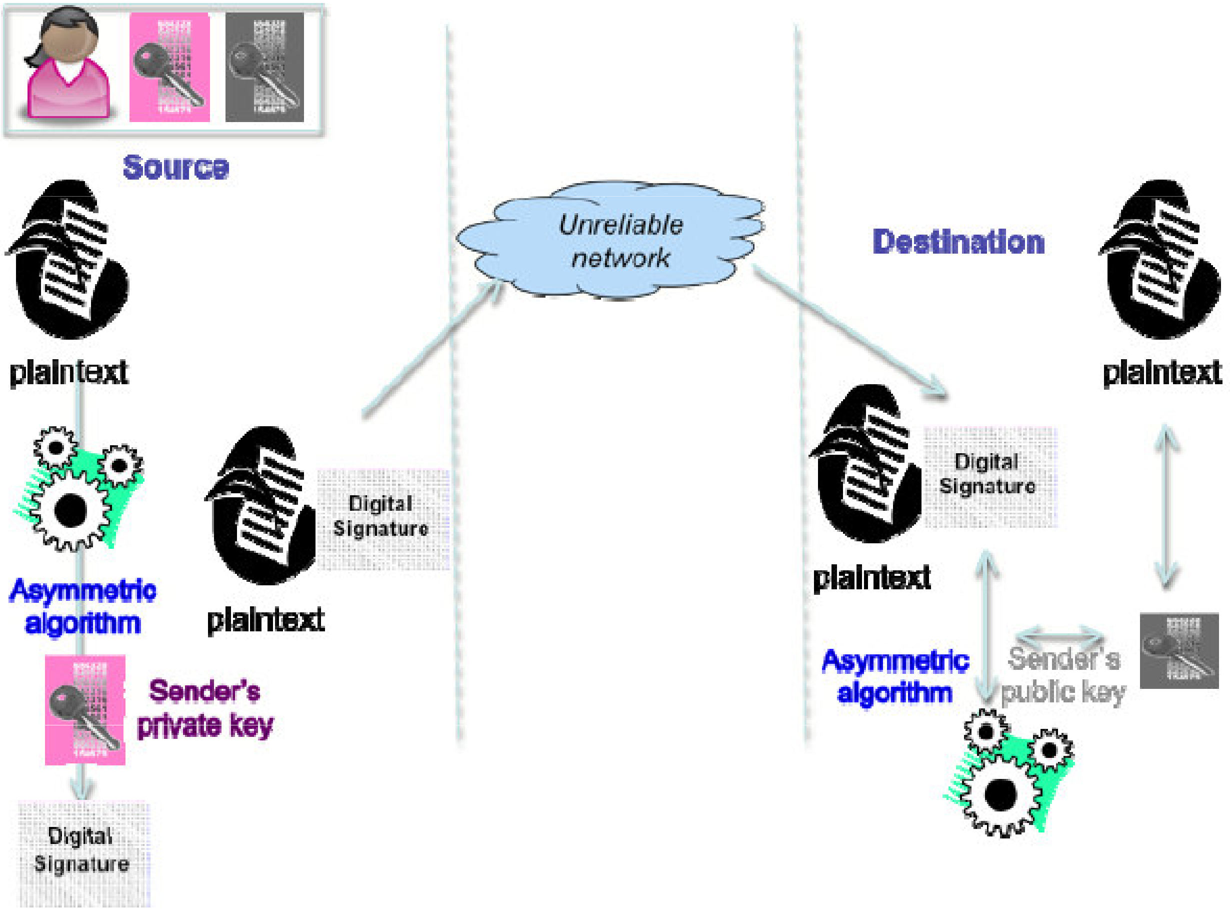
Figure II.9: Phishing attack

Keyloggers: Hardware & Software

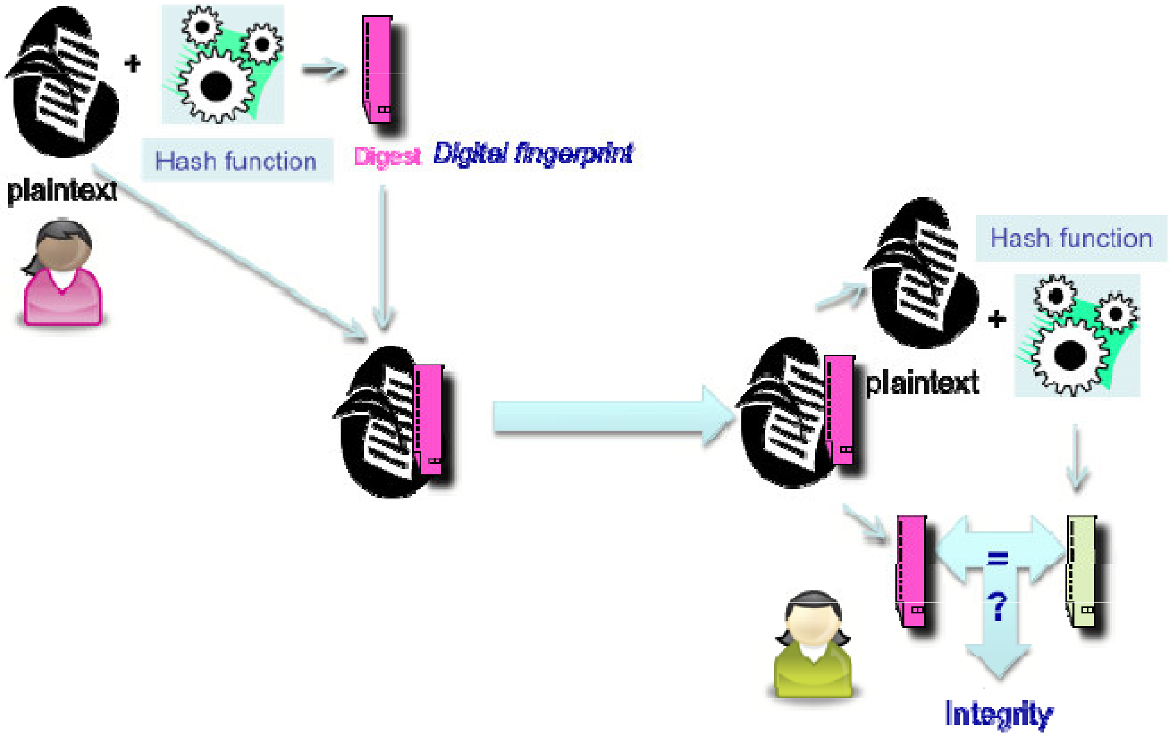
- Easily inserted by cybercriminals into PC wiring
- Wireless Versions also available for 802.11 nets
- Alternative software keyloggers can be illegally downloaded into compromised servers & PCs
- Logged files can be uploaded to cybercriminals through email or by FTP through open ports
- Examples have also been found inside credit card terminals, pre-installed by criminals in production plants with SIM Card and Phone. Log reports, including CC details and PINs are then regularly dialed through to overseas criminals



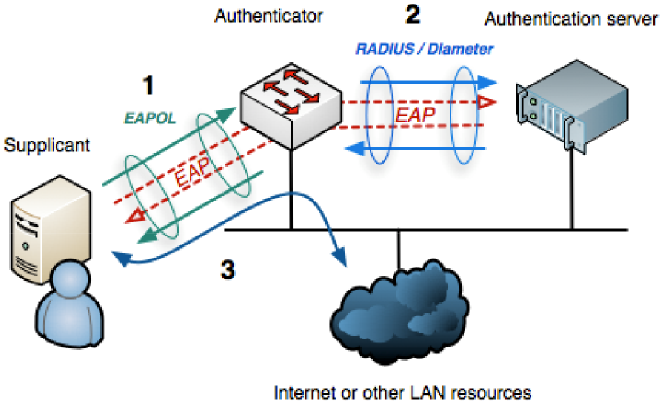
Digital Signature Transmission



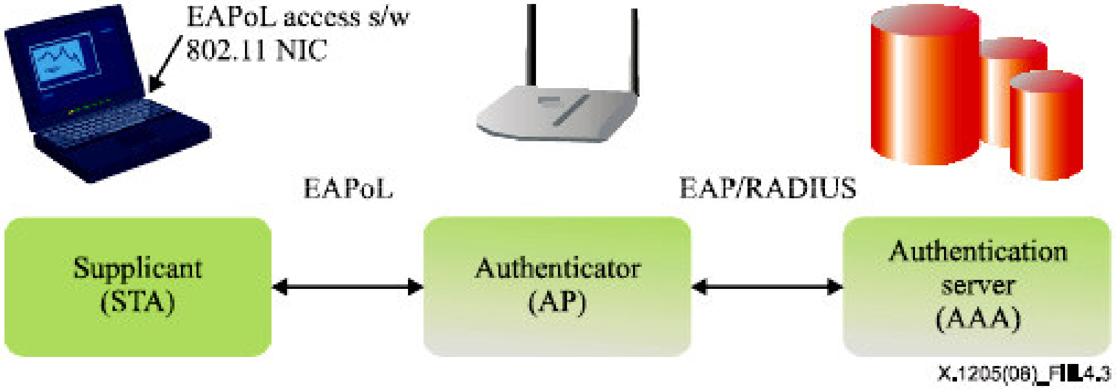
Digital Fingerprint Identification



Device Authentication with IEEE 802.1X



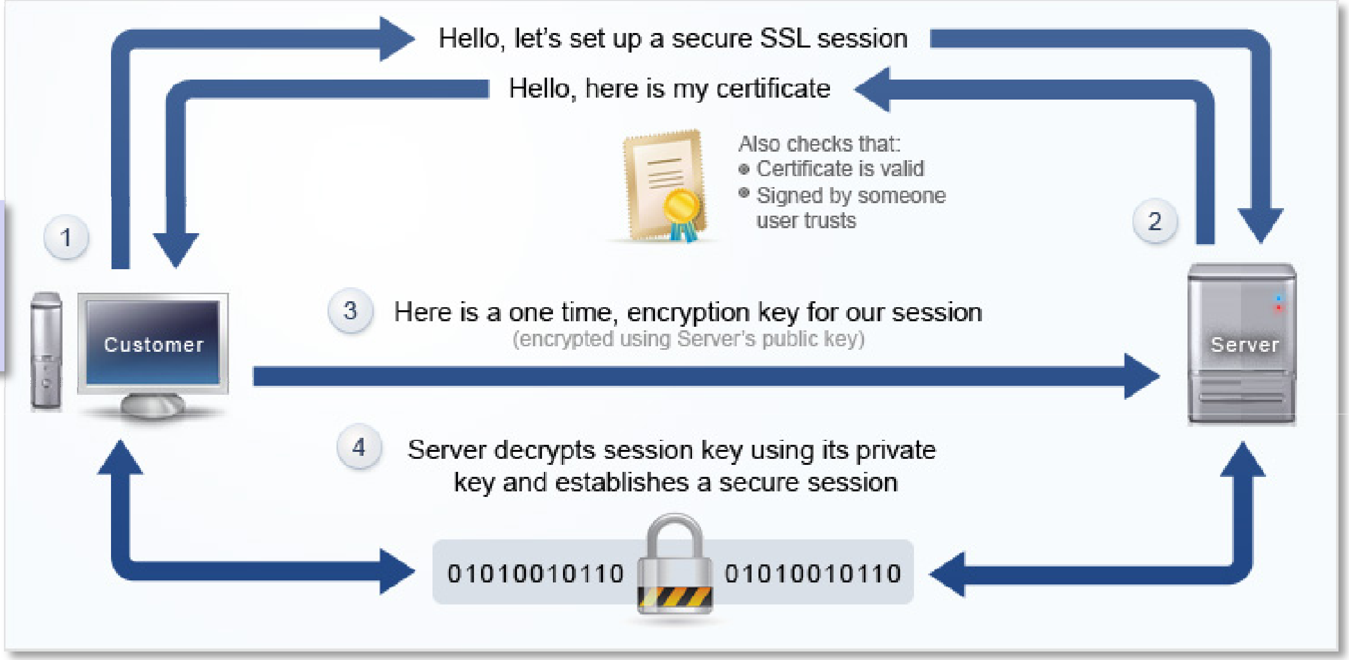
Extensible Authentication Protocol – EAP over IEEE 802.11 LAN/WLAN



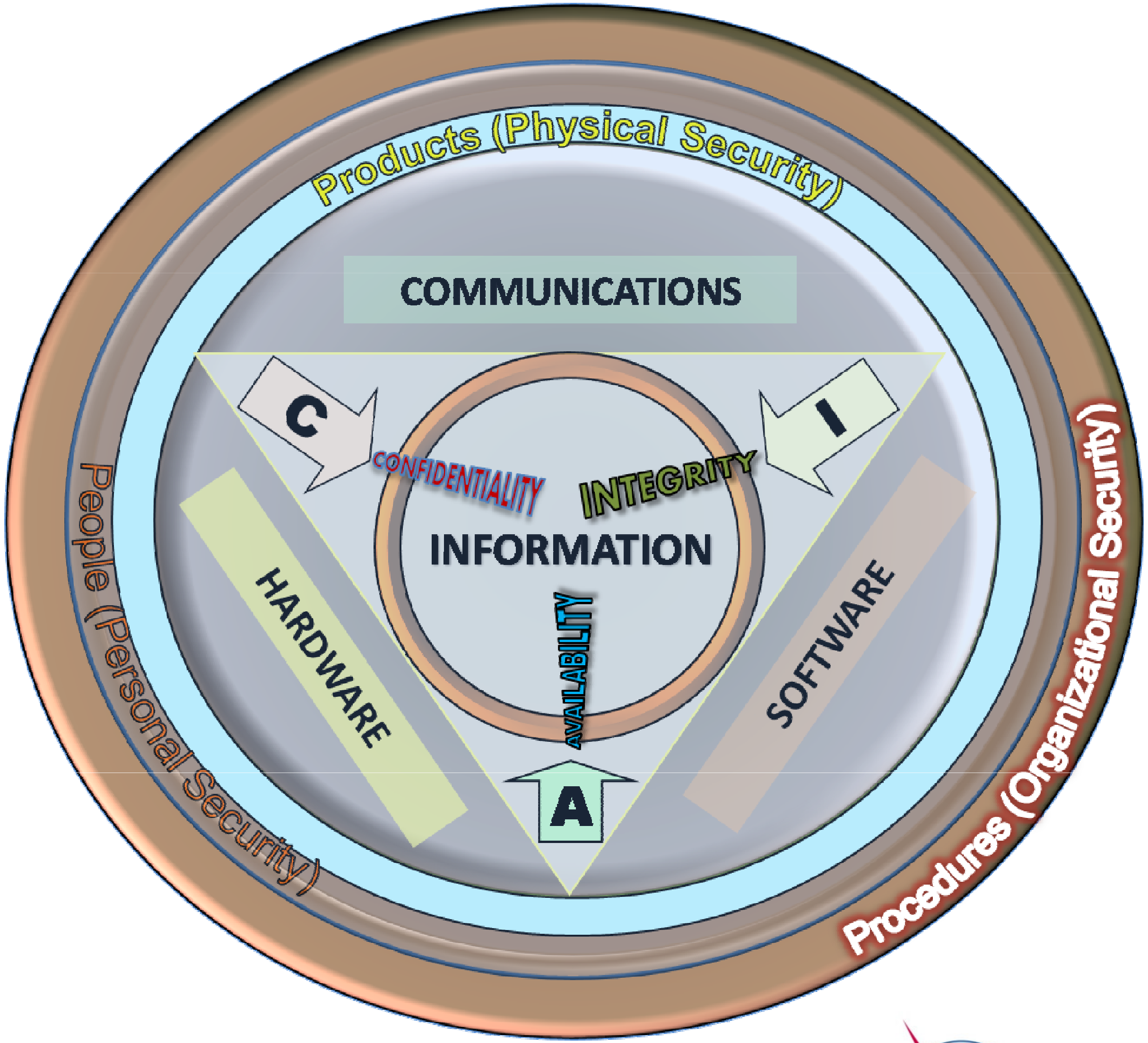
Transaction Security

- Transaction Security is required at each level of the Network Protocol
- Every Device and End-User should be authenticated by the network
- Both Public (PKI) and Private Key Encryption Schemes can be used
- Most Governments and Enterprises will generally adopt some form of Public Key Infrastructure to secure eGov and eBusiness Application

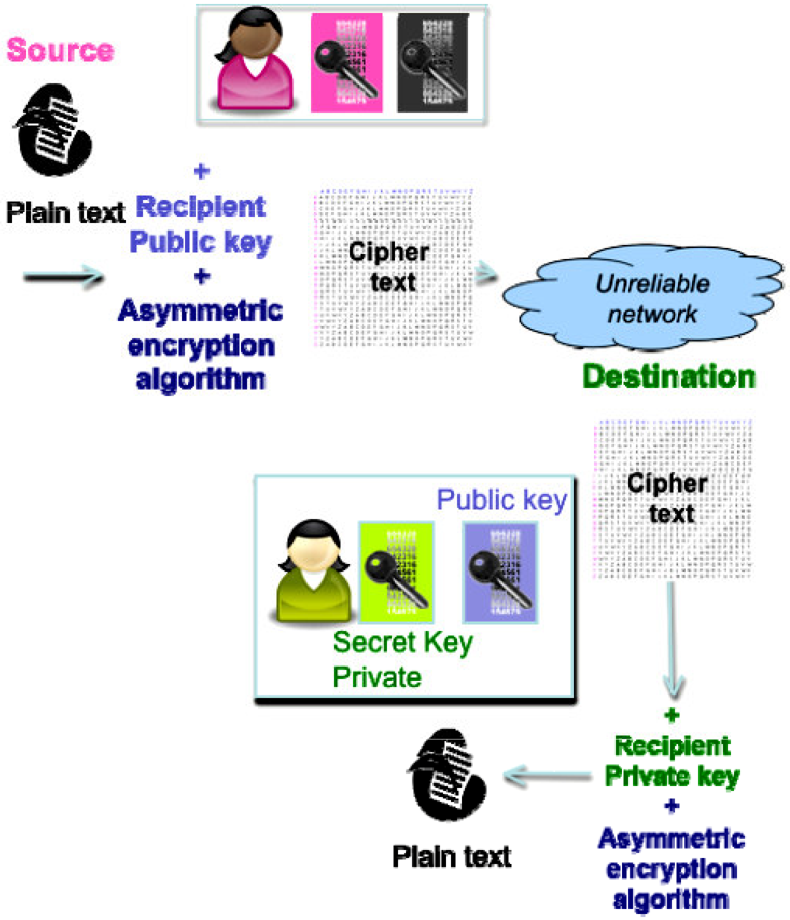
Example: SSL Secure Socket Layer Certificate and Private Key Encryption for Transactions


Hello, let's set up a secure SSL session
Hello, here is my certificate
Also checks that:
• Certificate is valid
• Signed by someone user trusts
1
2
Customer
Server
3
Here is a one time, encryption key for our session
(encrypted using Server's public key)
4
Server decrypts session key using its private key and establishes a secure session
01010010110
01010010110

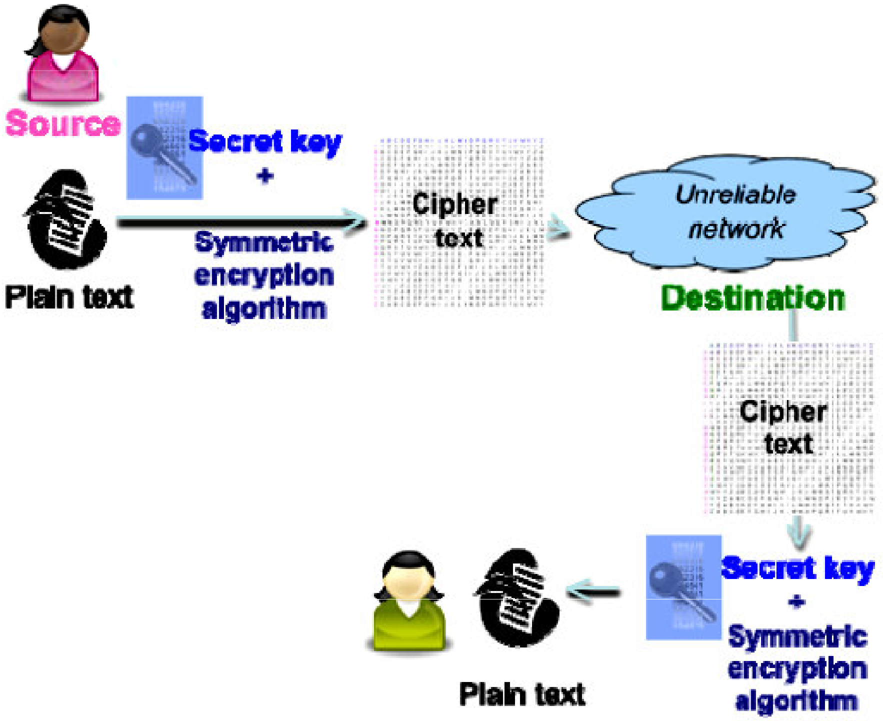
"Confidentiality, Integrity and Availability"


Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
AVAILABILITY
A
HARDWARE
SOFTWARE
People (Personal Security)
Procedures (Organizational Security)

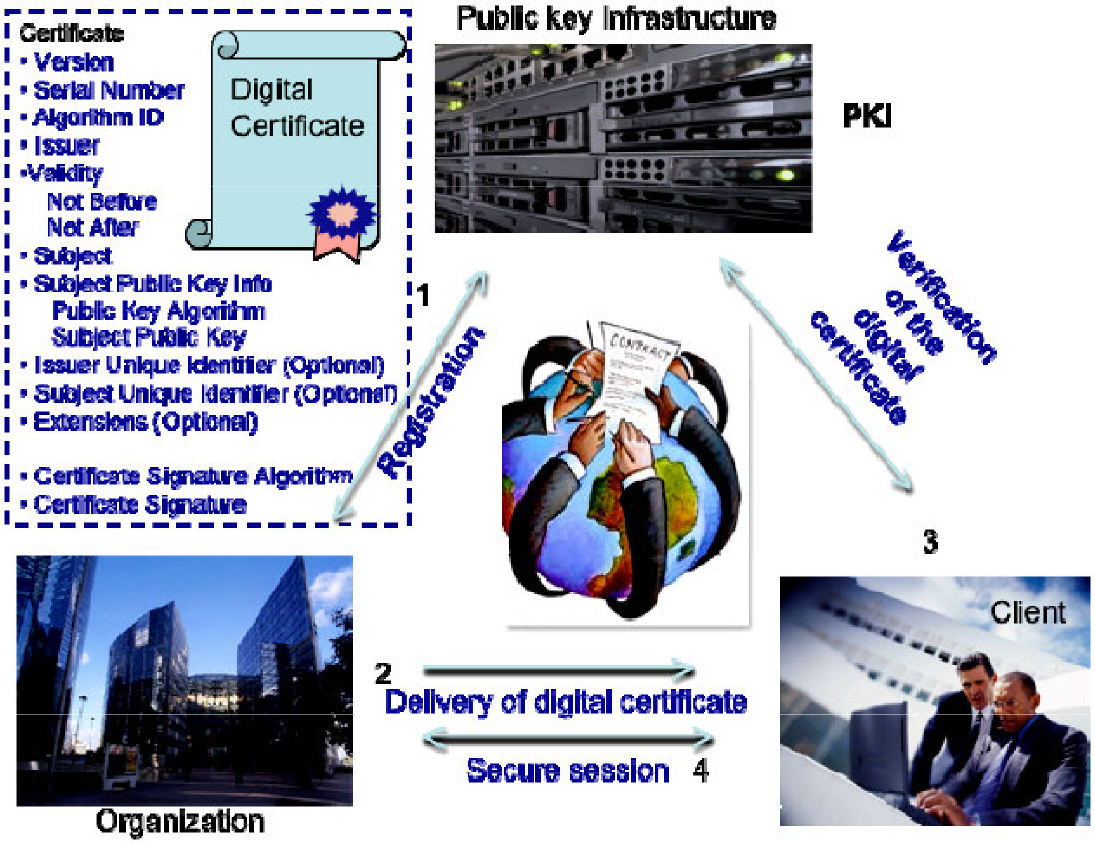
Public Key Encryption Scheme



Private Key Encryption Scheme



Cryptography: Public Key Infrastructure (PKI)



Certificate
- Version
- Serial Number
- Algorithm ID
- Issuer
- Validity
  - Not Before
  - Not After
- Subject
- Subject Public Key Info
  - Public Key Algorithm
  - Subject Public Key
- Issuer Unique Identifier (Optional)
- Subject Unique Identifier (Optional)
- Extensions (Optional)
- Certificate Signature Algorithm
- Certificate Signature

Digital Certficate
Public key Infrastructure
PKI
1
Registration
Verification of the digital certificate
3
2
Delivery of digital certificate
Secure session
4
Client
Organization

Figure IV.6: Public key infrastructure

*Workshop Session 2 *

"Integrated Cyber-Technological Solutions for the 21stC Web2.0 World"

1 – The 21stC Cyber World	2 – ITU Global CyberAgenda	3 – Cyber Technical Solutions:A
4 – Cyber Technical Solutions:B	5–Physical Security Solutions:A	6–Physical Security Solutions:B
7 – "Cyber to Physical Attacks"	8 – "Physical to Cyber Attacks"	9–Integrated Security Benefits

Cyber Technical Solutions (B)

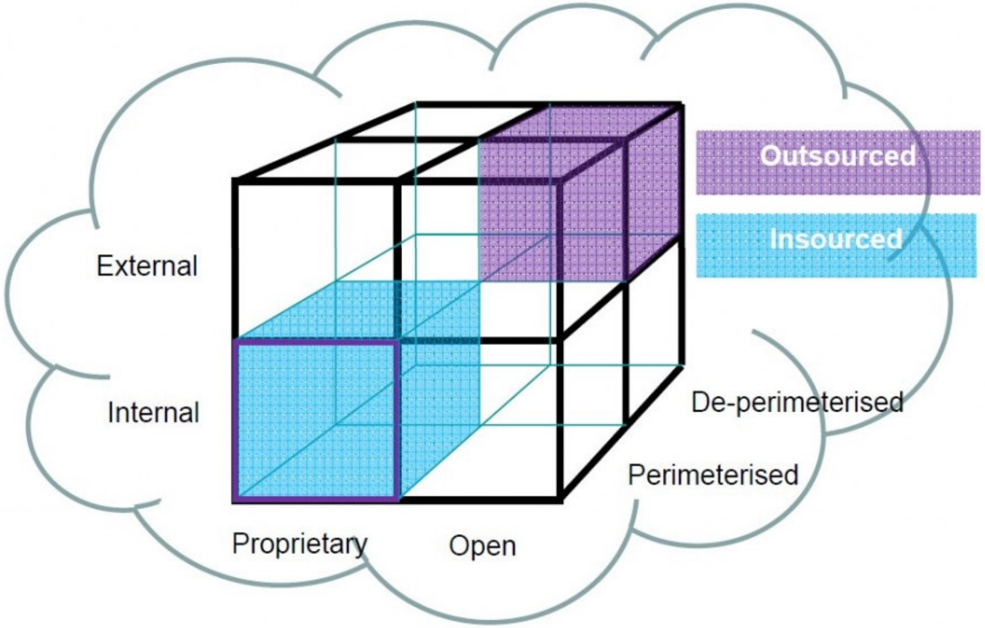
- Next we consider the more general aspects of 21stC Cybersecurity needs for evolving Enterprise ICT networks & applications:

  - Cybersecurity for Cloud Computing
  - Cybersecurity for System Virtualisation
  - Web2.0 "Apps" and Social Networking
  - Cybersecurity for Wireless Networks
  - Intrusion Detection & Prevention Systems (IDS/IPS)

……The *Virtual World of Cyberspace* is akin to the "real-world" in that cybercriminals will continuously develop "new weapons" to attack the national critical infrastructure, institutions and commercial organisations for financial gain & for political propaganda.

…There is also the concept of *"territorial gain"* in that the cybercriminals will also infect ICT devices and servers in order to secure control, and thence to use them as "zombie" bots

Cybersecurity for Cloud Computing



- "Cloud Cube Model" from the "Jericho Forum" which is a useful model for exploring cybersecurity "within the de-perimeterised world of cloud computing"
- Essentially all the same security technologies and operational procedures are applicable "within the cloud" and is just an extension of Web2.0 & open world ICT

Cybersecurity for Virtualisation

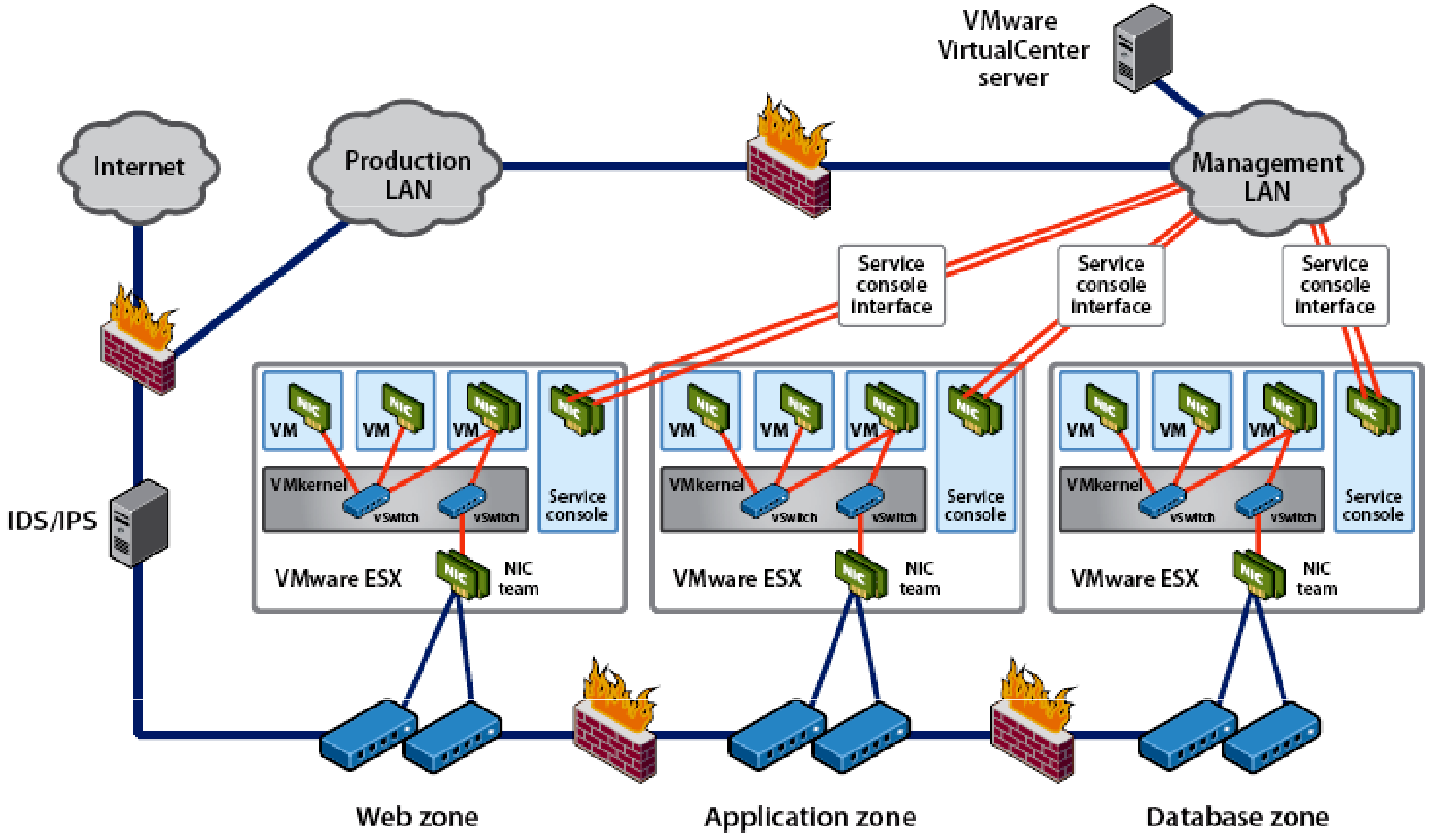


Figure 3 — Partially collapsed DMZ with separate physical trust zones

Fully Virtualised DMZ Firewalls

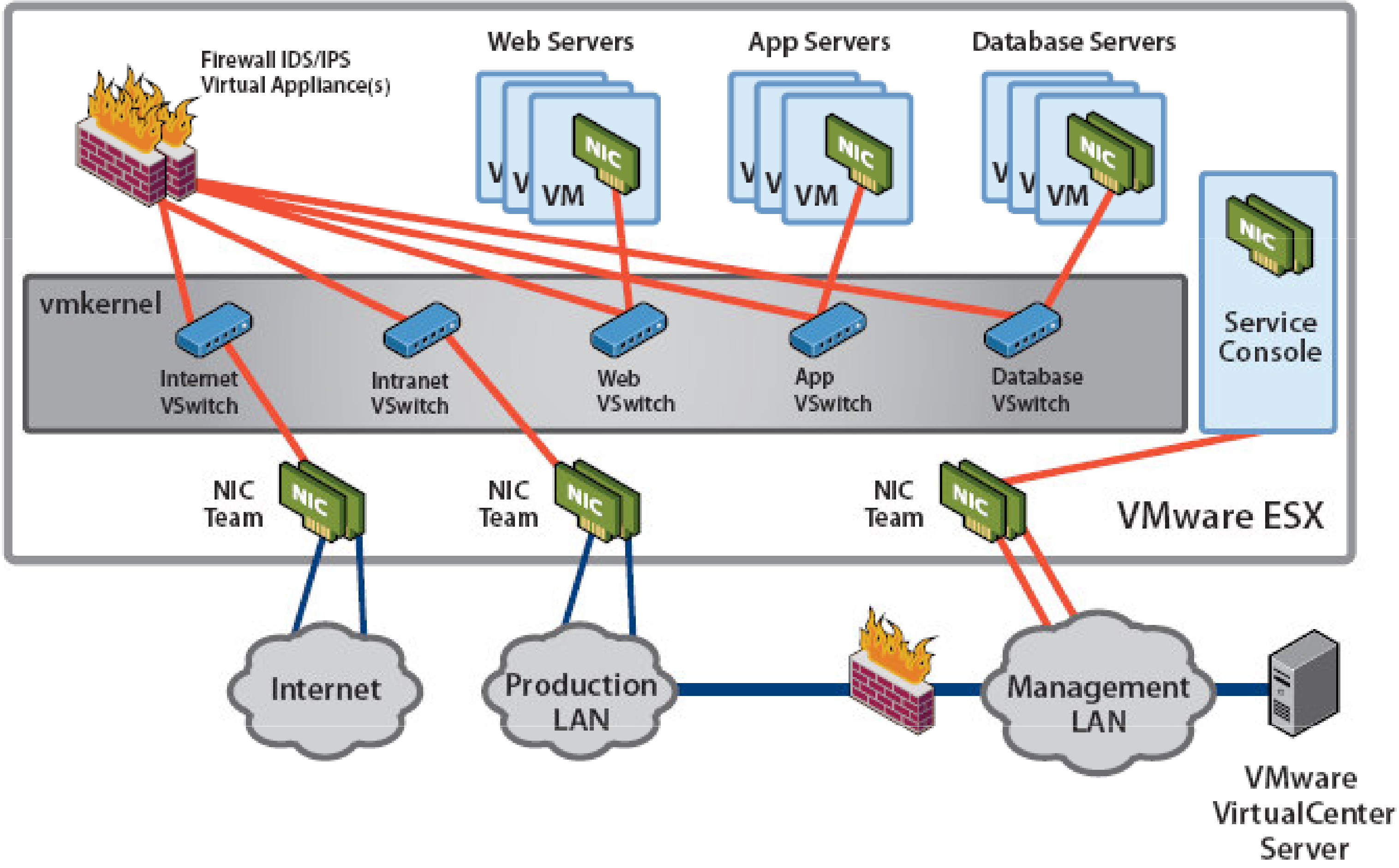


Figure 5 — Fully collapsed DMZ

Cybersecurity for Social Networks

- *Social Sites:* During the last 2 years, social networking sites such as Facebook and Myspace have become the latest targets for cybercriminals
- *Cyber Scams* include Identify Theft and requests for instant money transfers from parents to support the "release" of children & friends overseas
- *Cybercriminals* also sign-up as "friends" in order to infiltrate student networks, and then to secure personal information & account details
- *Paedophiles* also use these social networks in order to cultivate relationships with children and teenagers below the "age of consent"
- *Businesses* may be at risk if employees publish confidential company information on their social network accounts that may easily go public
- *Facebook* now works with child protection authorities in countries such as a the UK so that those at risk can quickly contact "helplines"

………Business and Government should consider ways to exploit the power of social networking whilst protecting their networks against attack.

Cybersecurity for Wireless Networks

- *Perimeter* Sentry Wireless Access Point Network around office/campus
- *Certificates:* End-User Encrypted Logon Certificates – EAP/802.1X
- *24/7 Scanning:* Permanent Wireless Frequency Sentry Scanning
- *Prohibition* of attachment of personal wireless nodes
- *3G Gadgets:* Management of Business PDAs and Smart Mobile Devices
- *Guests:* All guest account access either fully secured or prohibited
- *3G Mobiles:* Sensitive government or business data should always be encrypted and transmitted using secure VPN tunnel to home servers

Sentry Wireless Access Points for Building Perimeter Security

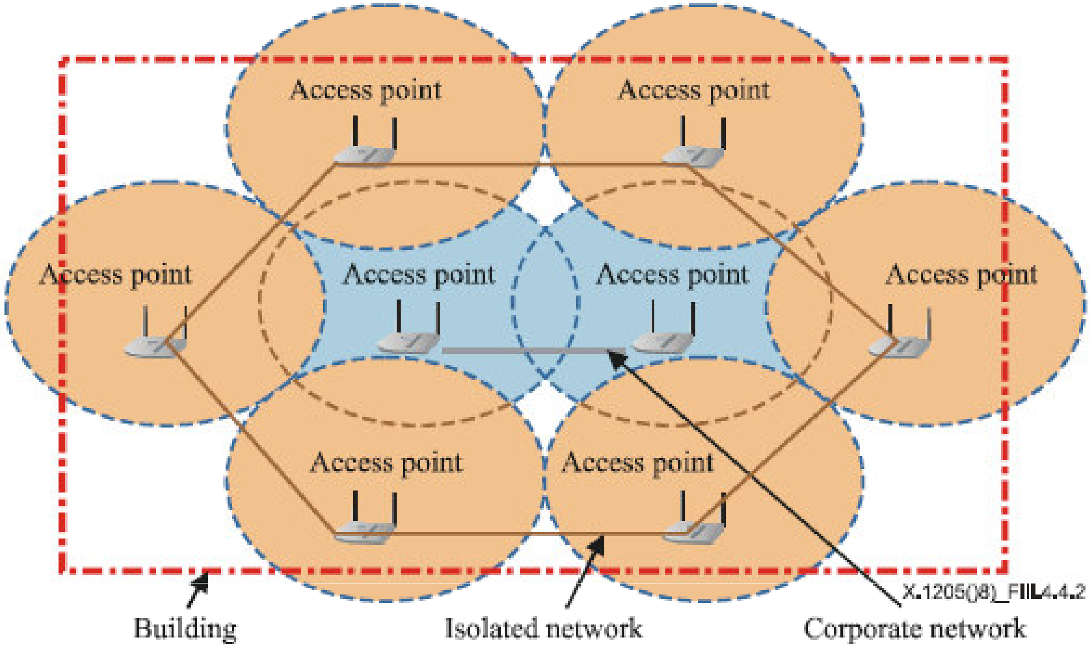
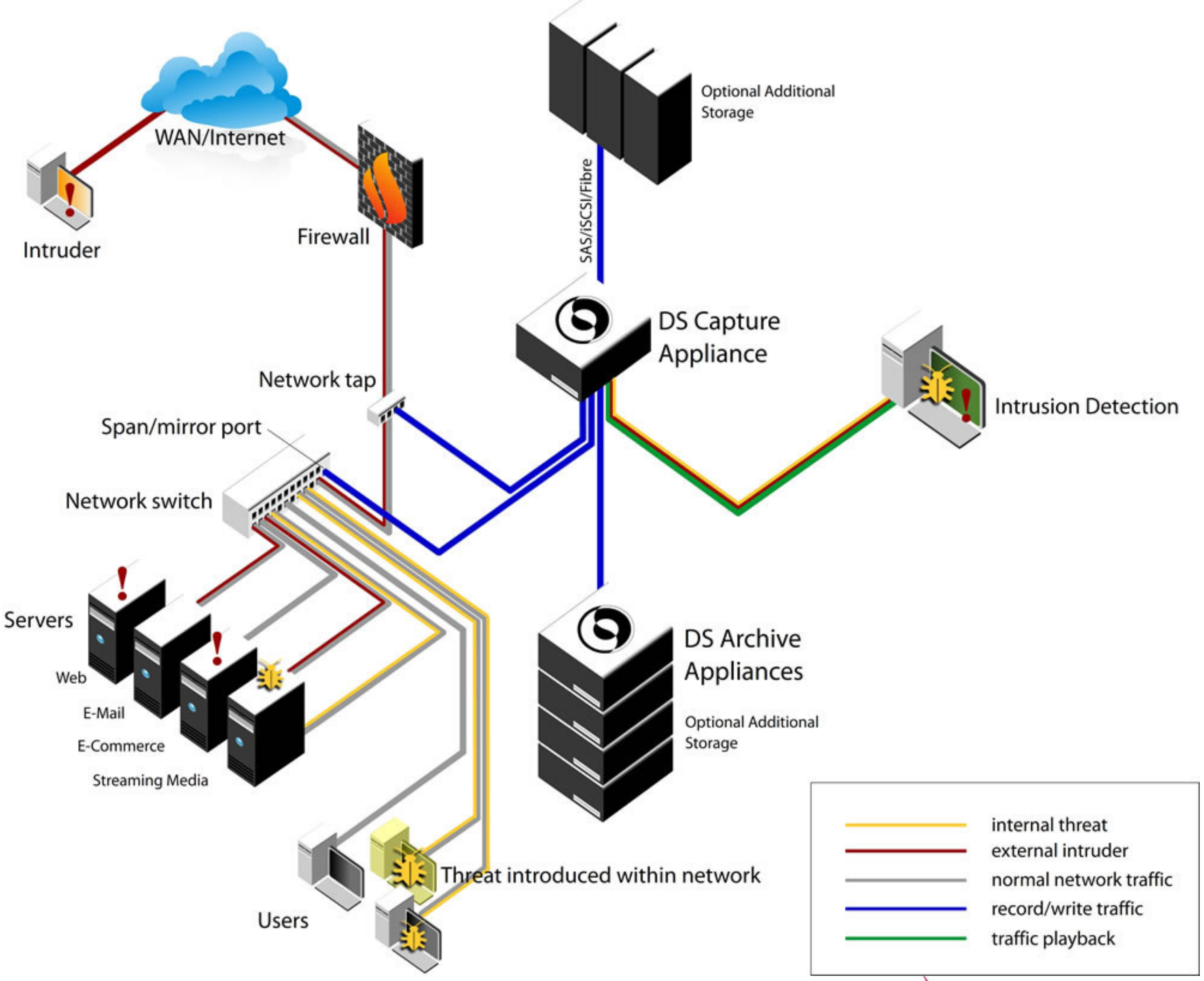


Figure III.4.4.2 – Sentry APs for perimeter security

IDS/IPS: Intrusion Detection and Prevention System



SECURITY OBJECTIVE	CYBERSECURITY TECHNOLOGY	SOLUTION ROLE
Access Control		
Boundary Protection	Firewalls	Aim to prevent unauthorised access to or from a private network.
	Content Management	Monitor web, messaging and other traffic for inappropriate content such as spam, banned file types and sensitive or classified information.
Authentication	Biometrics	Biometric systems rely on human body parts such as fingerprints, iris and voice to identify authorised users
	Smart tokens	Devices such as smart cards with integrated circuit chips (ICC) to store and process authentication details
Authorisation	User Rights and Privileges	Systems that rely on organisational rules and/or roles to manage access
System Integrity		
	Antivirus and anti-spyware	A collection of applications that fight malicious software (malware) such as viruses, worms, Trojan Horses etc
	Integrity Checkers	Applications such as Tripwire that monitor and/or report on changes to critical information assets
Cryptography		
	Digital Certificates	Rely on Public Key Infrastructure (PKI) to deliver services such as confidentiality, authentication, integrity and non-repudiation
	Virtual Private Networks	Enable segregation of a physical network in several ‘virtual’ networks
Audit and Monitoring		
	Intrusion Detection Systems (IDS)	Detect inappropriate, incorrect or abnormal activity on a network
	Intrusion Prevention Systems (IPS)	Use IDS data to build intelligence to detect and prevent cyber attacks
	Security Events Correlation Tools	Monitor, record, categorise and alert about abnormal events on network
	Computer Forensics tools	Identify, preserve and disseminate computer-based evidence
Configuration Management and Assurance		
	Policy Enforcement Applications	Systems that allow centralised monitoring and enforcement of an organisation’s security policies
	Network Management	Solutions for the control and monitoring of network issues such as security, capacity and performance
	Continuity of Operations tools	Backup systems that helps maintain operations after a failure or disaster
	Scanners	Tools for identifying, analysing and reporting on security vulnerabilities
	Patch Management	Tools for acquiring, testing and deploying updates or bug fixes

*Workshop Session 2 *

"Integrated Cyber-Technological Solutions for the 21stC Web2.0 World"

1 – The 21stC Cyber World	2 – ITU Global CyberAgenda	3 – Cyber Technical Solutions:A
4 – Cyber Technical Solutions:B	5–Physical Security Solutions:A	6–Physical Security Solutions:B
7 – "Cyber to Physical Attacks"	8 – "Physical to Cyber Attacks"	9–Integrated Security Benefits

Physical Security & Surveillance Solutions

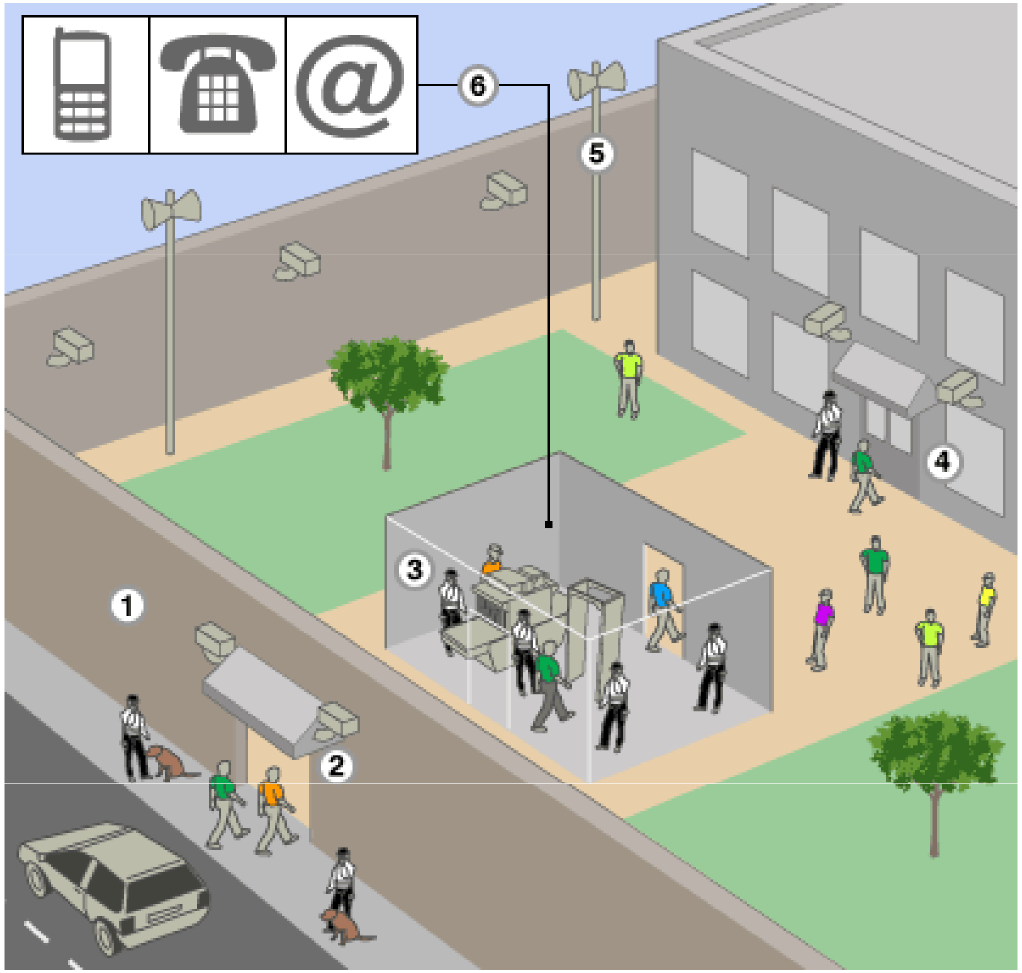
- The comprehensive security of electronic information, data and assets also requires corresponding upgrades in the physical & operational security for the offices, facilities and ICT server & storage rooms:

  - *Reception, Facility and Office Access* for Staff, Contractors and Visitors
  - *Advanced Smart Perimeter Management* for Campus Sites, Airports & Bases
  - *Integrated CCTV/ANPR* Intelligence Surveillance
  - *Biometrics and RFID* Identification for Personnel and Mobile Assets

……Traditionally physical security was managed quite independently from the ICT security. However, many enterprises and governments now understand that overall security is improved at lower cost through the integrated management of cyber & physical resources

Office, Facility and Campus Security

- All Facilities with Critical Info and ICT Infrastructure should be fully secured for access.
- Reception Security may include scanning devices, and policy for Mobiles, Laptops, Cameras and Memory to be left at reception.
- Site should be equipped with smart CCTV surveilliance
- All Staff and Guests have Smart Chip RFID Cards, and possibly also BioID Cards for facilities with higher security ratings.



Advanced Perimeter Management

- Critical Infrastructure such as Airports, Power Stations, Ports and Telecommunications Facilities are often sited on large multi-building campuses with a significant physical perimeter fence.

- Modern 21stC Technology can help to secure the perimeter, & prevent access to the electronic cyber assets within the facility:
  - Networked CCTV including Smart Video Analytics for Object Identification
  - Thermal Imaging and Movement Location with HD InfraRed Cameras
  - Optical Fibres for Real-Time Intrusion Location using EM Field Analysis
  - Buried Networked Wired or Wireless Motion Detection Sensors
  - ANPR Vehicle Registration Number Plate Recognition for Perimeter Roads
  - Professional Security Guards that are fully trained & certified in these Security Applications

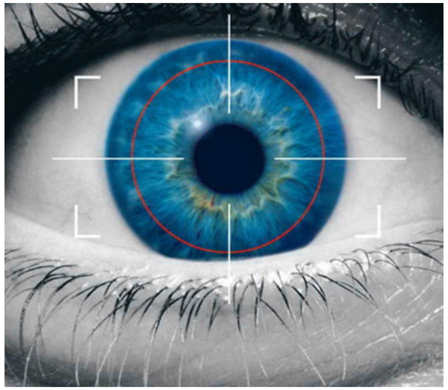
…In summary, it is important never to neglect upgrading investment in physical security in order to boost the security of ICT cyber assets

Integrated CCTV/ANPR Surveillance

Computer Automated Industrial Control & Safety Systems

Biometrics and RFID

- *Biometrics* techniques may include:
  - Finger and Palm Prints
  - Retinal and Iris Scans
  - 3D Vein ID
  - Voice Scans & Recognition
  - DNA Database – usually for Criminal Records
  - 3D Facial Recognition



- *RFID*= Radio Frequency ID with applications that include:
  - Personal ID Cards for Building, Facility and Secure Room Access
  - Tags for Retail Articles as a deterrence to shopplifting
  - Powered RFID Tags for Vehicles to open Barriers, Doors, or switch traffic lights
  - Plans to used RFID Tags for Perishable Products such as vegetables and flowers
  - Asset Tags to manage the movement of ICT Assets such as Laptops, PDA & Storage

…..Both Biometrics and RFID Technology Solutions can be powerful tools against cybercrime

*Workshop Session 2 *

"Integrated Cyber-Technological Solutions for the 21stC Web2.0 World"

1 – The 21stC Cyber World	2 – ITU Global CyberAgenda	3 – Cyber Technical Solutions:A
4 – Cyber Technical Solutions:B	5–Physical Security Solutions	6–Physical Security Solutions:B
7 – "Cyber to Physical Attacks"	8 – "Physical to Cyber Attacks"	9–Integrated Security Benefits

Operational Security Solutions

- Securing information and assets in the virtual world of cyberspace requires the discipline of rigorous operational security solutions and policies in the real-world according to accepted ITU & ISO Standards:

  - Integrated Command and Control Operations (including fail-over control rooms)
  - Business Continuity & Disaster Recovery (for cybercrimes, terrorism & natural disasters)
  - Implementation of National, and Enterprise Computer Incident Response Teams (CERTs)
  - Integrated Digital Forensics, eCrime Unit & Cyber Legislation against Cybercrimes
  - Traditional Physical Security Defences & Deterrents (including security guards & fences!

….Many criminal and terrorist attacks are through penetrating some combination of physical and cybersecurity systems. Breaking into a physical building may allow a criminal to gain secure ICT zones, and thence to on-line user accounts, documents & databases. Information can be downloaded to chips or storage drives & stolen with relative ease.

……We'll be considering some real-world examples of cybercriminal "integrated cyber-physical security threats" in the next part of our cyber technology workshop

Integrated Command & Control Operations

- Security Operations Command Centre for Global Security Software Enterprise

TSA National Operations Room: US Transportation Security Administration

Business Continuity and Disaster Recovery Plans

Disaster Scenarios

Business Continuity Plan BCP

Business Impact Analysis BIA

Contingency Concept

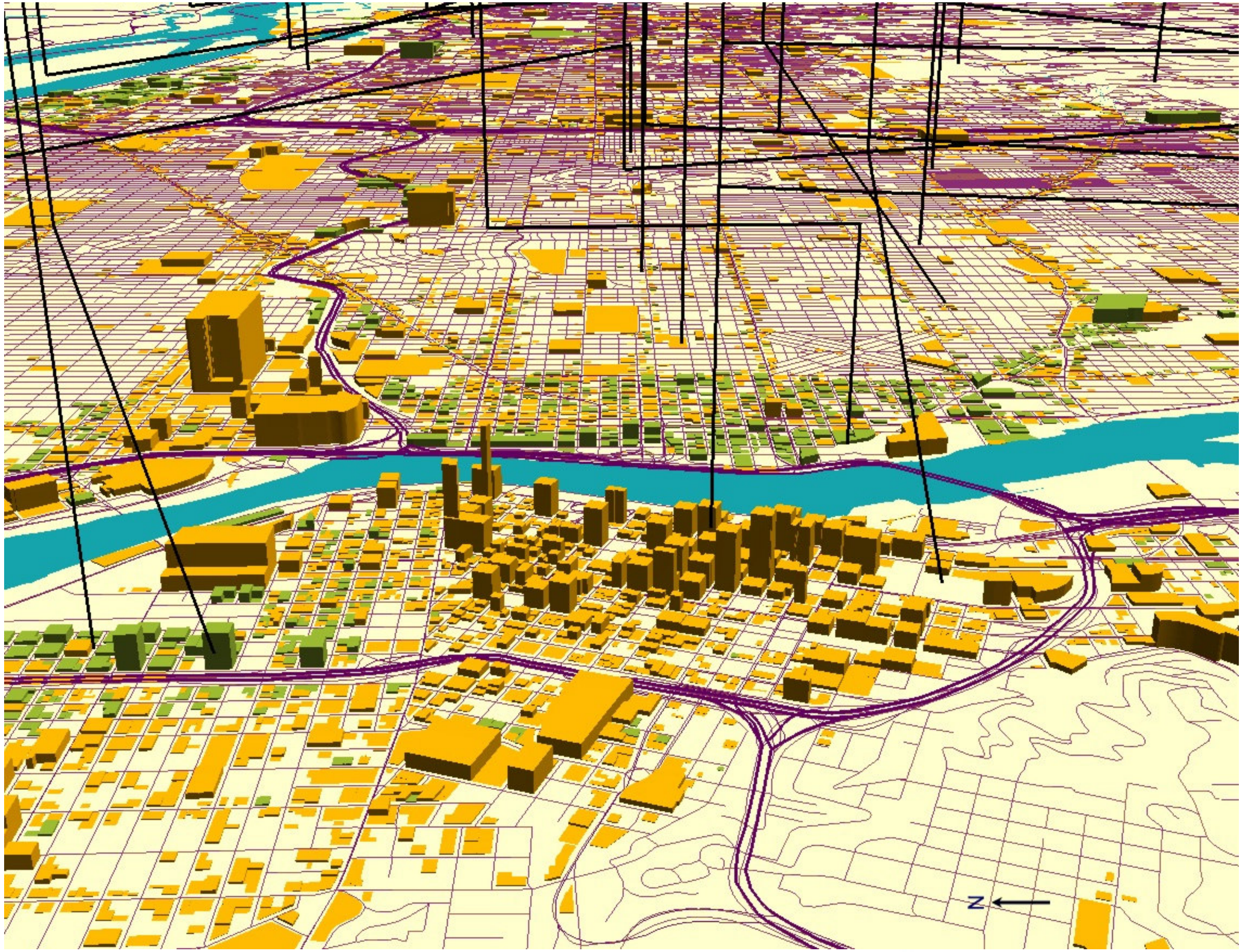
Spans ALL aspects of Operations both Physical And Cyber Operations

Emergency Plan Business

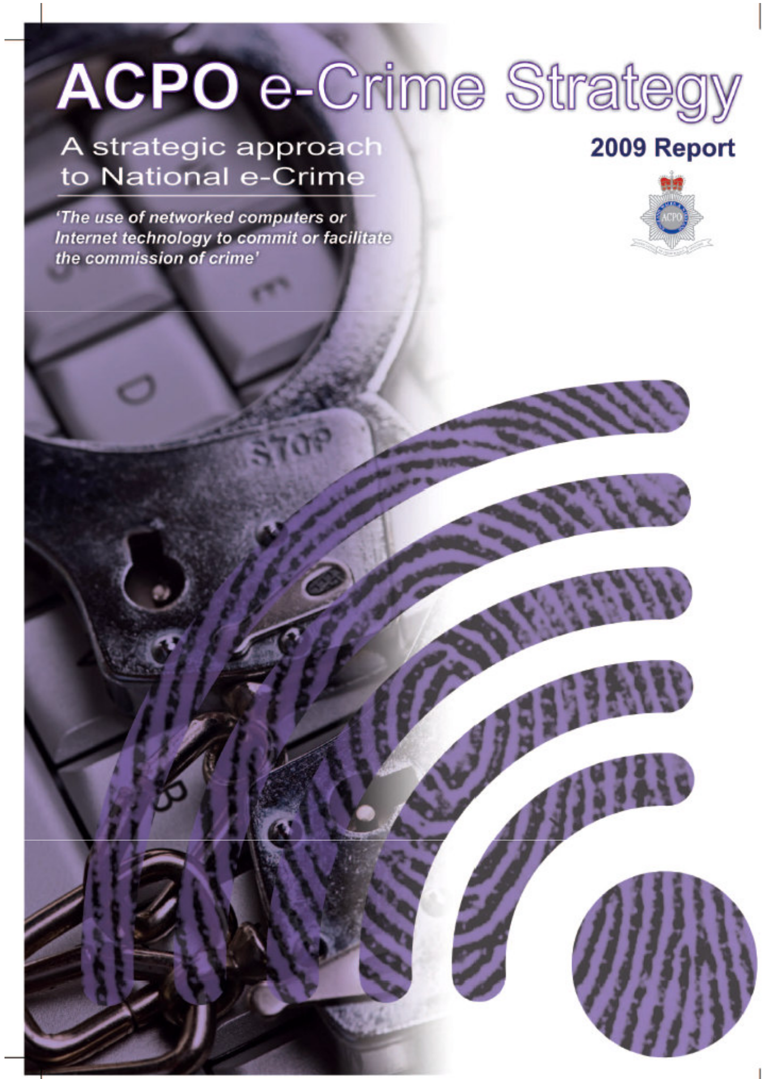
Emergency plans Buildings/Infrastructure

IT Disaster Recovery Plan

3D Simulation Modelling for Security Crisis & Disaster Management



Strategic Approach to National e-Crime Unit

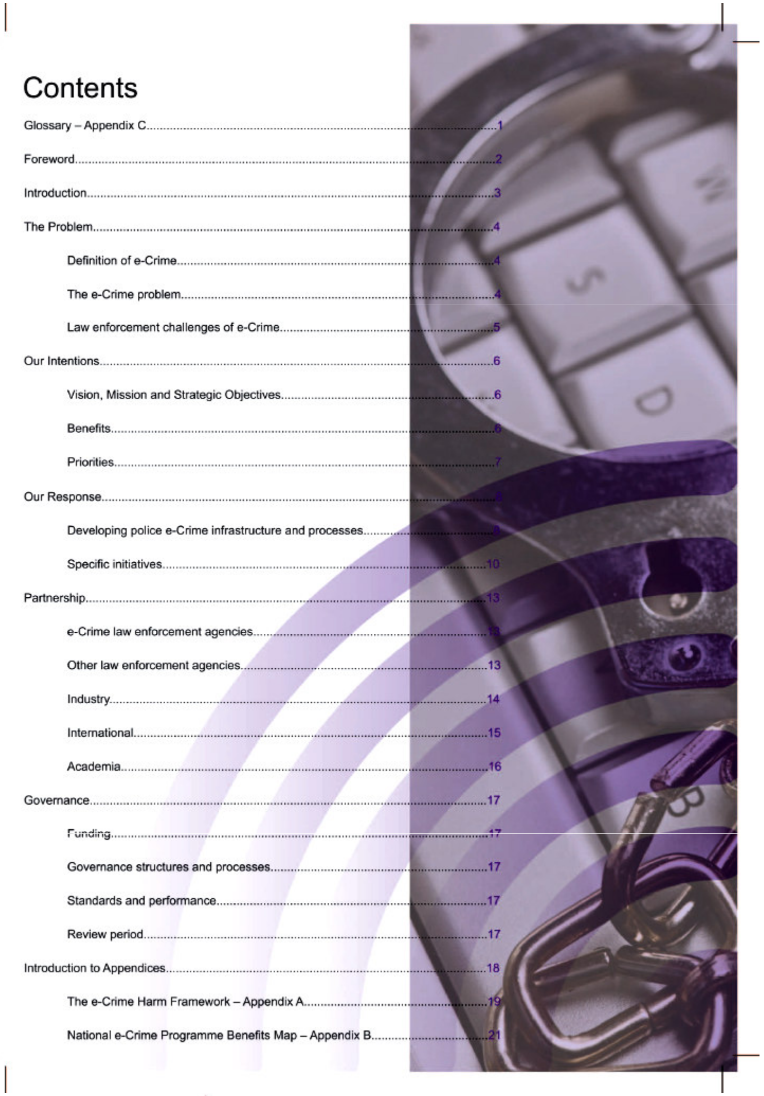


ACPO e-Crime Strategy

A strategic approach
to National e-Crime

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

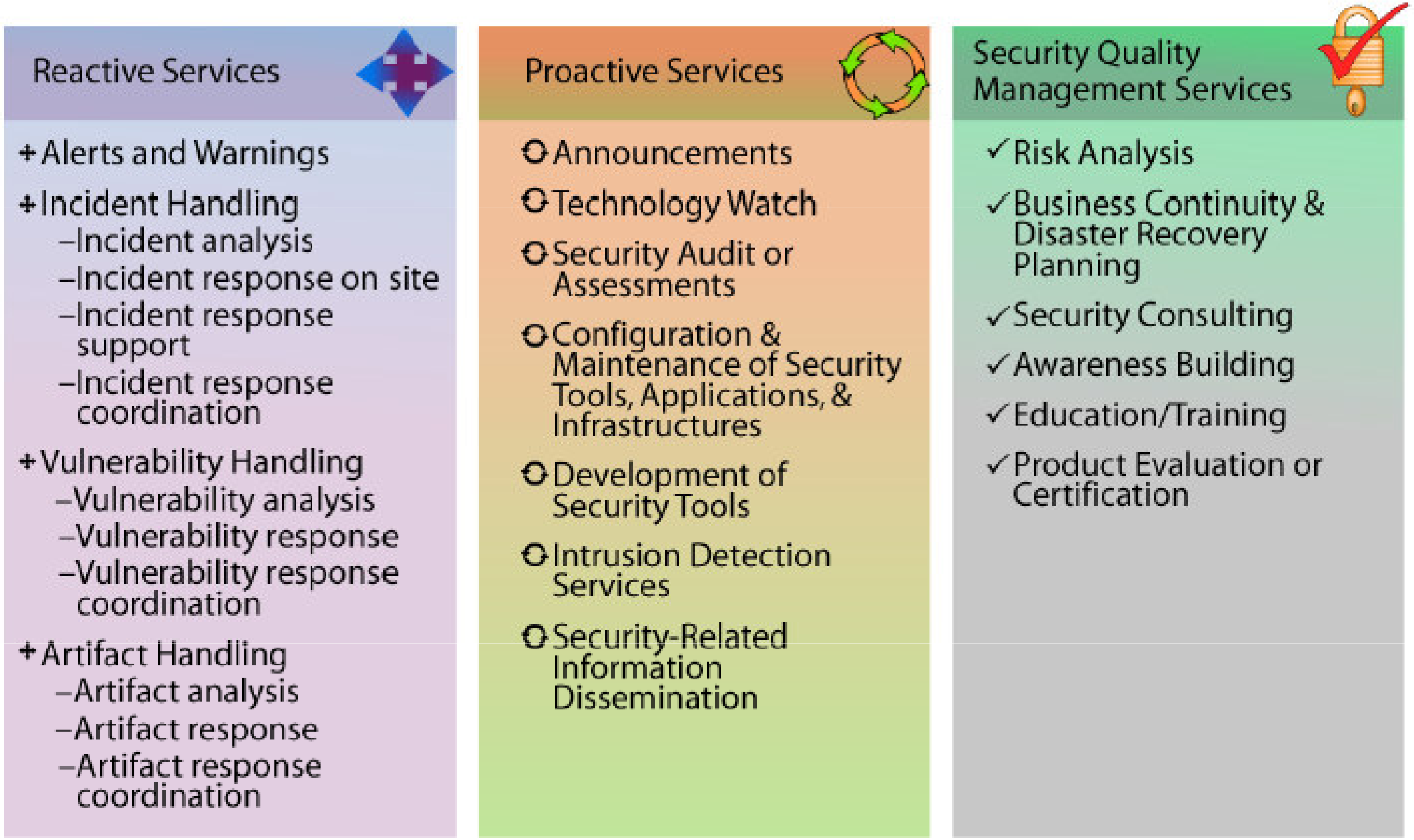
2009 Report



Contents

Glossary – Appendix C........1
Foreword........2
Introduction........3
The Problem........4
Definition of e-Crime........4
The e-Crime problem........4
Law enforcement challenges of e-Crime........5
Our Intentions........6
Vision, Mission and Strategic Objectives........6
Benefits........6
Priorities........7
Our Response........8
Developing police e-Crime infrastructure and processes........8
Specific initiatives........10
Partnership........13
e-Crime law enforcement agencies........13
Other law enforcement agencies........13
Industry........14
International........15
Academia........16
Governance........17
Funding........17
Governance structures and processes........17
Standards and performance........17
Review period........17
Introduction to Appendices........18
The e-Crime Harm Framework – Appendix A........19
National e-Crime Programme Benefits Map – Appendix B........21

Implemention of CERT/CSIRT Services



Reactive Services

- + Alerts and Warnings
- + Incident Handling
  - –Incident analysis
  - –Incident response on site
  - –Incident response support
  - –Incident response coordination
- + Vulnerability Handling
  - –Vulnerability analysis
  - –Vulnerability response
  - –Vulnerability response coordination
- + Artifact Handling
  - –Artifact analysis
  - –Artifact response
  - –Artifact response coordination

Proactive Services

- ○ Announcements
- ○ Technology Watch
- ○ Security Audit or Assessments
- ○ Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- ○ Development of Security Tools
- ○ Intrusion Detection Services
- ○ Security-Related Information Dissemination

Security Quality Management Services

- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

“Physical Security” Defences in the context of “Cybersecurity”

- Investments in establishing and upgrading cybersecurity defences against cybercrime means that all physical security and associated operational staff should also be reviewed for compliance with policies, and audited to international standards

- Ideally, physical and cybersecurity operations should be linked “step-by-step” at the command and control level in the main facility operations centre.

- Physical Security for critical service sectors such as airports, banks, telecomms, energy, education, healthcare and national defence should be included within the strategy and policies for Cybersecurity and vice versa

- In order to maximise security, Jamaican Government and Businesses need to upgrade and integrate resources and plans for both physical and cybersecurity during the next few years.

- I would personally suggest developing a focused total security action plan and roadmap (Physical & Cyber) for each critical sector within the Jamaican Economy

Physical Security Defences: Berlin-Schönefeld Airport

Summary of Physical Security and Operational Solutions

- Physical security and the Operational Solutions are increasingly based upon sophisticated electronic networked solutions, including biometrics, smart CCTV, intelligent fences, and RFID Access Devices

- Operations for “Physical Security” and “Cybersecurity” will need to be slowly converged & integrated during the next few years both from a personnel, assets, resources and operational budget perspective

- The benefits of integrating cyber and physical security are reduced running costs, reduced penetration risk, and increased early warning of potential attack whether from criminals, hackers or terrorists.

…..Next we’ll consider the integration of physical and cybersecurity in some more detail, including the modes of attack & overall benefits

*Workshop Session 2 *

"Integrated Cyber-Technological Solutions for the 21stC Web2.0 World"

1 – The 21stC Cyber World	2 – ITU Global CyberAgenda	3 – Cyber Technical Solutions:A
4 – Cyber Technical Solutions:B	5–Physical Security Solutions:A	6–Physical Security Solutions:B
7 – "Cyber to Physical Attacks"	8 – "Physical to Cyber Attacks"	9–Integrated Security Benefits

“Cyber to Physical Attacks”

- The illegal penetration of ICT systems may allow criminals to secure information or “make deals” that facilities their real-world activities:
  - *“Sleeping Cyber Bots”* – These can be secretly implanted by skilled hackers to secure on-line systems, and programmed to explore the directories & databases, and & then to transmit certain information – Account & Credit Card Details, Plans, Projects, Deals
  - *Destructive “Cyber Bots”* – If cyber-bots are implanted by terrorist agents within the operational controls of power plants, airports, ports or telecomms facilities then considerable physical damage may result. A simple *“delete *.*”* command for the root directories would instantly wipe out all files unless the facility has real-time fail-over!
  - *Distributed Denial of Service Attacks* – These not only block access to system, but in the case of a Banking ATM Network, means that the national ATM network has to be closed. Alternatively in the case of an airline check-in and dispatch system, flights are delayed.
  - *National CyberAttacks* – Many international organisations such as NATO & US DOD forecast that future regional conflicts will begin with massive cyberattacks to disable their targets’ physical critical communications and information infrastructure. Clearly it is important for countries to upgrade their national cybersecurity to minimise such risks

*Workshop Session 2 *

"Integrated Cyber-Technological Solutions for the 21stC Web2.0 World"

1 – The 21stC Cyber World	2 – ITU Global CyberAgenda	3 – Cyber Technical Solutions:A
4 – Cyber Technical Solutions:B	5–Physical Security Solutions:A	6–Physical Security Solutions:B
7 – "Cyber to Physical Attacks"	8 – "Physical to Cyber Attacks"	9–Integrated Security Benefits

“Physical to Cyber Attacks”

- Most “physical to cyber attacks” involve staff, contractors or visitors performing criminal activities in the “misuse of computer assets”:
  - *Theft & Modification of ICT Assets:* It is now almost a daily occurrence for critical information & databases to be either deliberately stolen or simply lost on PCs or Chips
  - *Fake Maintenance Staff or Contractors:* A relatively easy way for criminals to access secure facilities, particularly in remote regions or developing countries is to fake their personnel IDs and CVs as being legitimate ICT maintenance staff or contractors
  - *Compromised Operations Staff:* Sometime operational ICT staff may be tempted by criminal bribes, or possibly blackmailed into providing passwords, IDs & Access Codes.
  - *Facility Guests and Visitors:* It is standard procedure for guests & visitors to be accompanied at all times in secure premises. In the absence of such procedures, criminals, masquerading as guests or visitors, may install keylogger hardware devices or possibly extract information, plans and databases to USB memory chips, or steal DVDs!

*Workshop Session 2 *

"Integrated Cyber-Technological Solutions for the 21stC Web2.0 World"

1 – The 21stC Cyber World	2 – ITU Global CyberAgenda	3 – Cyber Technical Solutions:A
4 – Cyber Technical Solutions:B	5–Physical Security Solutions:A	6–Physical Security Solutions:B
7 – "Cyber to Physical Attacks"	8 – "Physical to Cyber Attacks"	9–Integrated Security Benefits

Benefits of Integrated Cybersecurity

- Some of the key benefits from integrating cybersecurity technology solutions with rigorous operational processes and policies are:

  - *Reduced Operational Costs*, through "Single Security Organisation" under a CSO/CISO
  - *Early Warning* of both Physical or Cyber Penetration through comprehensive surveillance
  - *Extended Protection* of ALL Critical Physical and On-Line Assets
  - *Focused Security Policy* for Government, Businesses and Citizens
  - *Risks:* Reduced "Open World" Security Risks from Smart Mobile Devices ,"Apps" & Web2.0
  - *CyberCrime:* Comprehensive Management and Control of National Cybercrime
  - *CNI:* Critical Infrastructure such as Banks, Power Stations and Airports are better protected
  - *National Defence:* Countries now need to be 100% protected both in physical & cyberspace

….In summary, the 21st approach to cybersecurity is a combination of technological solutions together with rigorously enforced operational procedures, all implemented to recognised international standards such as those of the ITU and ISO/IEC

….Tomorrow we consider these ITU cybersecurity standards in more depth, and also discuss specific organisational models for National CERTs/CSIRTs and Police eCrime Units

* ITU Workshop Overview*

"Cybersecurity Technologies, Standards & Operations"

S1-Thurs: 9:30-11:00 "The International Cybercrime and Cybersecurity Challenge"	S2–Thurs:11:30-13:00 "Integration Cyber-Technological Solutions for the 21stC Web2.0 World"	S3-Thurs:14:00-15:30 Group Session: "Securing Critical Computing and Network Facilities"	S4-Thurs:16:00-17:30 Group Session: "Group Discussion: Securing Critical Computing and Network Facilities"
S5 - Fri: 9:30–11:00 "Cybersecurity Continuity Planning, Standards and Architectures"	S6 – Fri: 11:30–13:00 "Organising a National Crime Unit and CERT/CSIRT"	S7 – Fri: 14:00-15:30 Group Session: "Designing Practical Cybercrime Solutions – Critical Sectors"	S7 – Fri: 16:00-17:30 Group Session" "Group Discussion: Designing Practical Cybercrime Solutions – Critical Sectors"

Cybersecurity: Director ITU Telecomms Development Bureau

> "Maintaining cybersecurity worldwide requires our constant attention and widespread cooperation. The ITU is working hard to provide useful resources and tools for countries to address their cybersecurity issues and specific needs, as well as to assist them in establishing Cybersecurity capabilities, and it is the feedback we receive from our Member States that will enable us to make those tools ever more useful."

Mr. Sami Al Morshid Al Basheer
Director, ITU Telecommunication
Development Bureau (BDT)

Group Workshop Session 3
"Securing Critical Computing & Network Facilities"

- Workgroup Team Task:

  - *Task 1* – Choose your critical sector: (1) Government, (2) Banking/Finance, (3) Telecomms/Mobile, (4) Energy/Power (5) Airport/Transportation

  - *Task 2* – Imagine that you're a cybercriminal or hacker and list all the possible technical & operational cyberthreats that could penetrate the sector

  - *Task 3* – Design your ICT computer facility (servers, databases, access, network)

  - *Task 4* – Check that your facility design can be defended against the list of potential cyberthreats that you listed under task 2 including both the technology threats and operational & staff related threats

  - *Task 5* – Develop a short presentation and slides to justify your facility design

……Position yourself as the CIO/CSO of your chosen Critical Sector ICT Facility!

* Group Workshop Session 3*
Securing Critical ICT Infrastructure
Suggested Time Allocations for Task Actions: 90mins

1 – Task Assignment: Choose your Critical Service Sector: ***Government, Banking/Finance Telecomms, Transport, Energy***	**Task 2 – List CyberThreats**	**Task 2 – List Cyberthreats**
Task 3 – Cybersecurity Design	**Task 3 – Cybersecurity Design**	**Task 3 – Cybersecurity Design**
Task 4 – Check Design against your List of Cyberthreats	**Task 5 – Prepare Short 10 Min Presentation of Design & Plan**	**Task 5 – Prepare Short 10min Presentation of Design & Plan**

Note: ***Each Task Time Segment = 10Mins***

Key to Cybersecurity Workshop Session Colour-Code Classifications: Interactive Tasks

Colour Code / Workshop	RED	ORANGE	YELLOW	BLUE	GREEN
Monday *-Action Plans -*	(1) Legal	(2) Technical	(3) Organisation	(4) Capacity	(5) International
Tuesday *- Laws -*	Information Disclosure	Computer Misuse	Forgery & ID Fraud	Information Interception	Copyright & Patents Law
Wednesday *- Road Map -*	Q1-2011	Q2-2011	Q3-2011	Q4-2011	FY2012
Thursday *- ICT Security-*	**Unauthorised Info Access**	**DDoS-Denial of Services**	**MALWARE**	**Disclosure & Misuse**	**Info Access & Exploitation**
Friday *- Sector Security -*	Cyber Criminal Threat	Cyber Terrorist Threat	Malicious Hacking & Exploitation	Internal Operational Threat	Natural Disaster or Other Event

* ITU Workshop Overview*

"Cybersecurity Technologies, Standards & Operations"

S1-Thurs: 9:30-11:00 "The International Cybercrime and Cybersecurity Challenge"	S2–Thurs:11:30-13:00 "Integration Cyber-Technological Solutions for the 21stC Web2.0 World"	S3-Thurs:14:00-15:30 Group Session: "Securing Critical Computing and Network Facilities"	S4-Thurs:16:00-17:30 Group Session: "Group Discussion: Securing Critical Computing and Network Facilities"
S5 - Fri: 9:30–11:00 "Cybersecurity Continuity Planning, Standards and Architectures"	S6 – Fri: 11:30–13:00 "Organising a National Crime Unit and CERT/CSIRT"	S7 – Fri: 14:00-15:30 Group Session: "Designing Practical Cybercrime Solutions – Critical Sectors"	S7 – Fri: 16:00-17:30 Group Session" "Group Discussion: Designing Practical Cybercrime Solutions – Critical Sectors"

* Group Workshop Session 4*
Team Discussion: Securing Critical ICT Infrastructure
Schedule: Task Presentations = 90mins

Group 1 = Government	Group 1 = Government	Group 2 = Banking/Finance
Group 2 = Banking/Finance	Group 3 = Telecomms/Mobile	Group 3 = Telecomms/Mobile
Group 4 = Transport or Energy	Group 4 = Transport or Energy	Group Discussion & Summary

Note: ***Each Task Time Segment = 10Mins***

Securing the Island of Jamaica!...
....From 17thC Coastline to 21stC Cyberspace

* ITU Workshop Overview*

"Cybersecurity Technologies, Standards & Operations"

S1-Thurs: 9:30-11:00 "The International Cybercrime and Cybersecurity Challenge"	S2–Thurs:11:30-13:00 "Integration Cyber-Technological Solutions for the 21stC Web2.0 World"	S3-Thurs:14:00-15:30 Group Session: "Securing Critical Computing and Network Facilities"	S4-Thurs:16:00-17:30 Group Session: "Group Discussion: Securing Critical Computing and Network Facilities"
S5 - Fri: 9:30–11:00 "Cybersecurity Continuity Planning, Standards and Architectures"	S6 – Fri: 11:30–13:00 "Organising a National Crime Unit and CERT/CSIRT"	S7 – Fri: 14:00-15:30 Group Session: "Designing Practical Cybercrime Solutions – Critical Sectors"	S7 – Fri: 16:00-17:30 Group Session" "Group Discussion: Designing Practical Cybercrime Solutions – Critical Sectors"

* Workshop Session 5 *

"Cybersecurity Continuity Planning, Standards and Architectures"

1 – International Standards	2 – ITU Security Standards	3 – ITU: X.805 Architecture
4 – ITU: X1205 CyberSecurity	5 – Others: ISO/IEC & NIST	6 – ISF: Info Security Forum
7 – Practical Implementation	8 – Cyber Continuity: BCP/DR	9 – Next Steps for Jamaica

* Workshop Session 5 *

"Cybersecurity Continuity Planning, Standards and Architectures"

1 – International Standards	2 – ITU Security Standards	3 – ITU: X.805 Architecture
4 – ITU: X1205 CyberSecurity	5 – Others: ISO/IEC & NIST	6 – ISF: Info Security Forum
7 – Practical Implementation	8 – Cyber Continuity: BCP/DR	9 – Next Steps for Jamaica

International Security Standards

- *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

- *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

* Workshop Session 5 *

"Cybersecurity Continuity Planning, Standards and Architectures"

1 – International Standards	2 – ITU Security Standards	3 – ITU: X.805 Architecture
4 – ITU: X1205 CyberSecurity	5 – Others: ISO/IEC & NIST	6 – ISF: Info Security Forum
7 – Practical Implementation	8 – Cyber Continuity: BCP/DR	9 – Next Steps for Jamaica

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

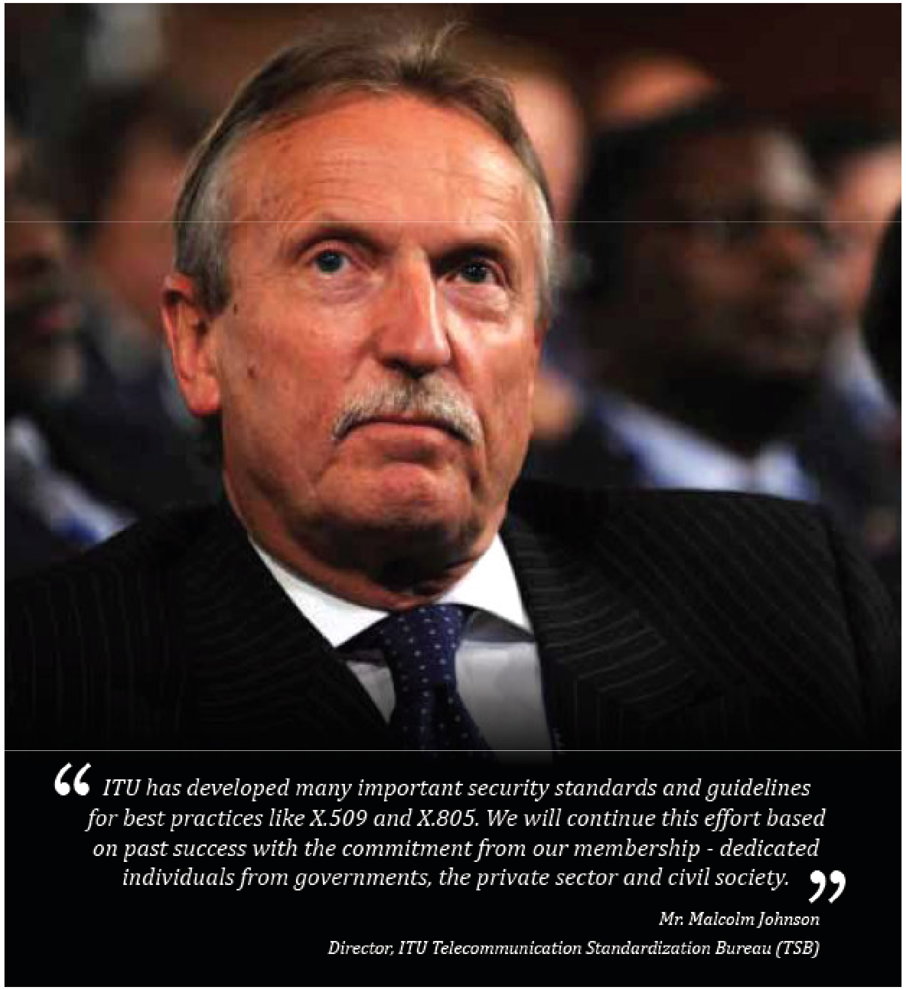
  - *X.805* – Security Architecture for End-to-End Communications
  - *X.1121* – Security Technologies for Mobile Data Communications
  - *X1191* – Functional Requirements for IPTV Security Agents
  - *X.1205* – Overview of Cybersecurity and General Guidelines
  - *X.1250* – Security Standards for Identity 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/**

Cybersecurity: Director, ITU Telecommunications Standardisation Bureau

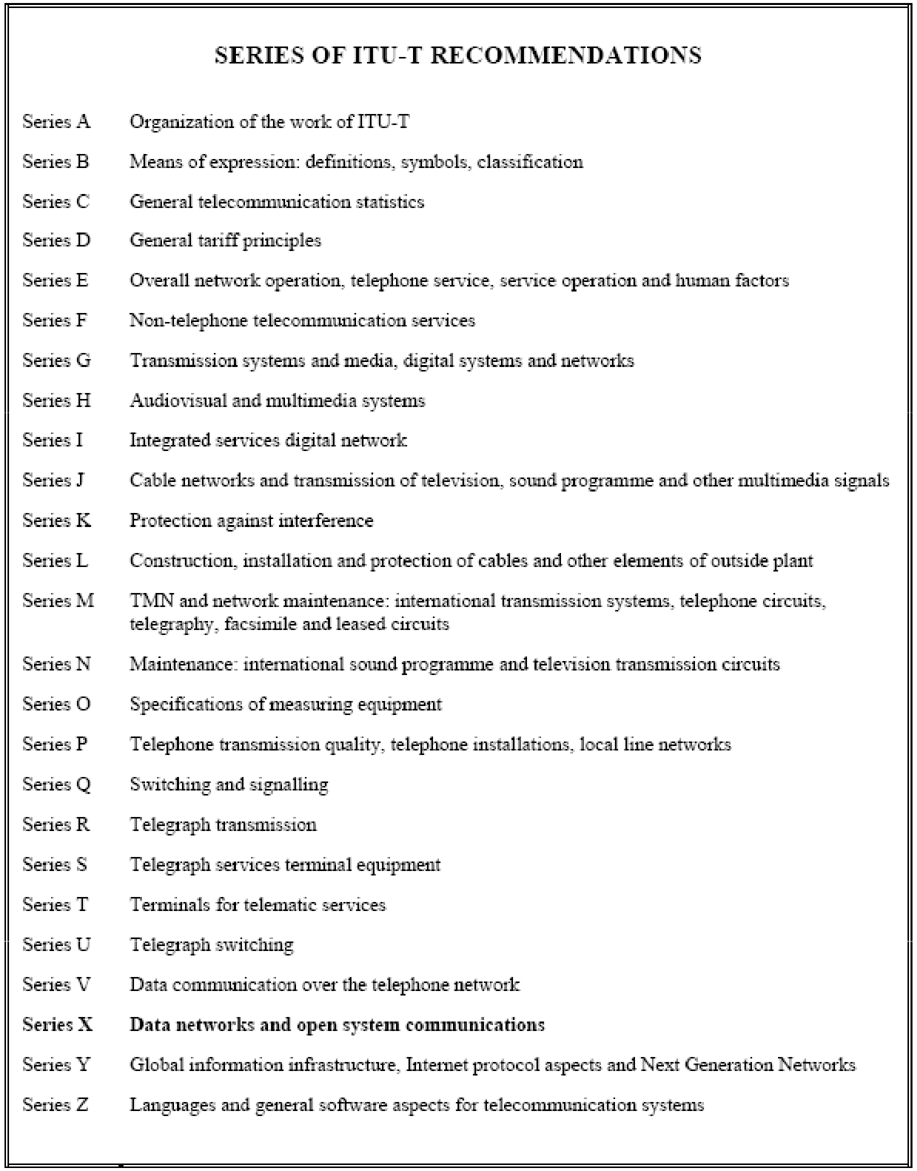


“ITU has developed many important security standards and guidelines for best practices like X.509 and X.805. We will continue this effort based on past success with the commitment from our membership - dedicated individuals from governments, the private sector and civil society.”

Mr. Malcolm Johnson

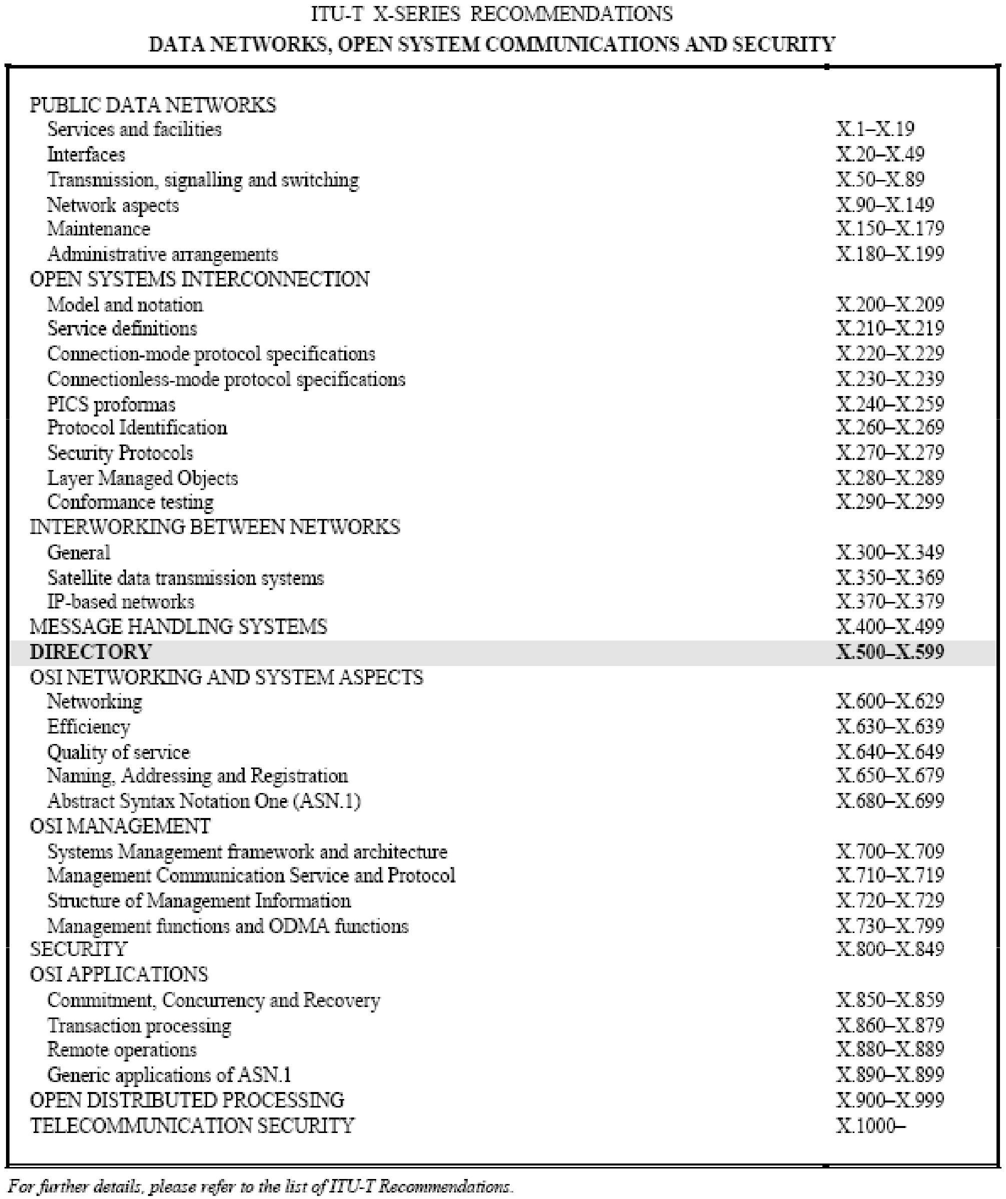
Director, ITU Telecommunication Standardization Bureau (TSB)

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–

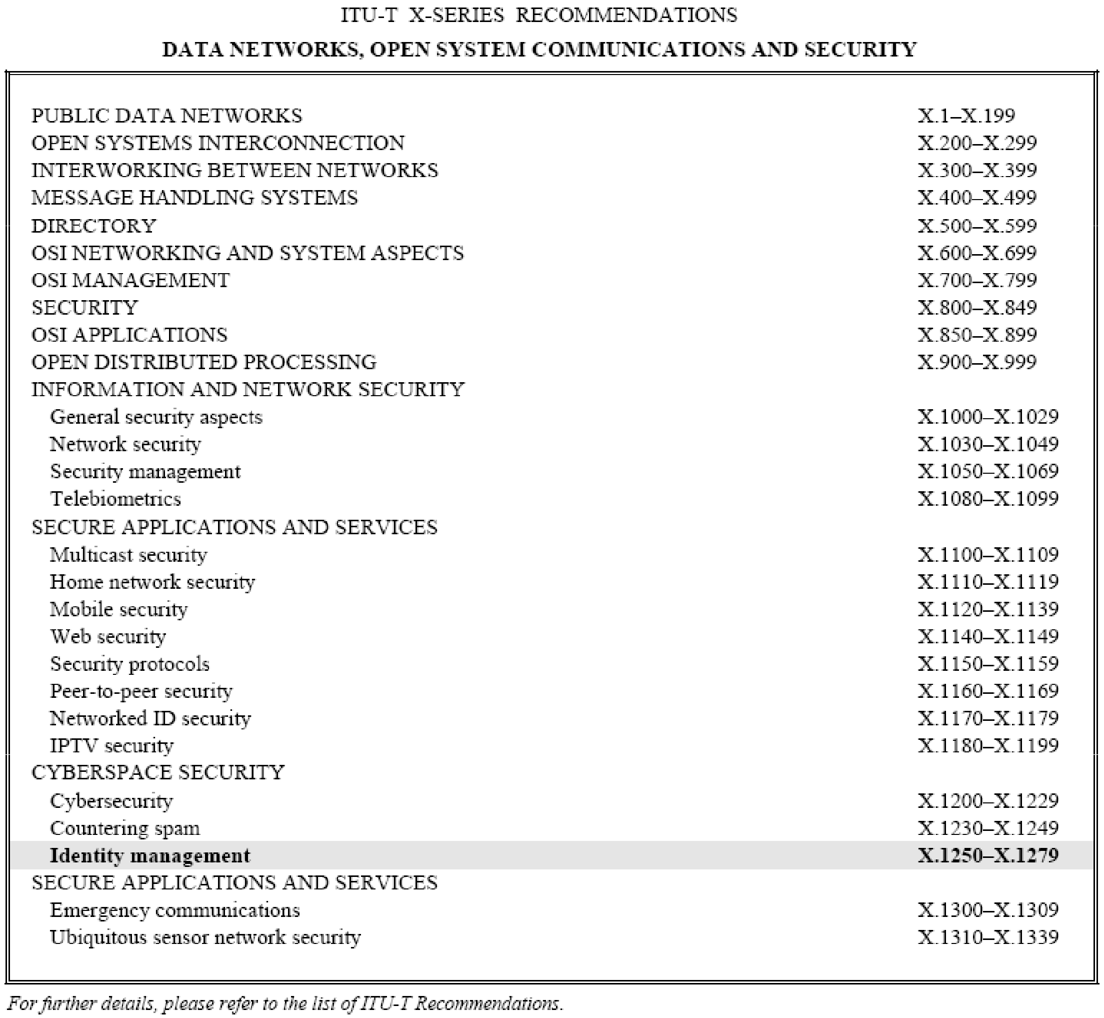
For further details, please refer to the list of ITU-T Recommendations.

University of Technology, Jamaica

International Telecommunication Union

Committed to connecting the world

ITU-T X-Series Security Recommendations



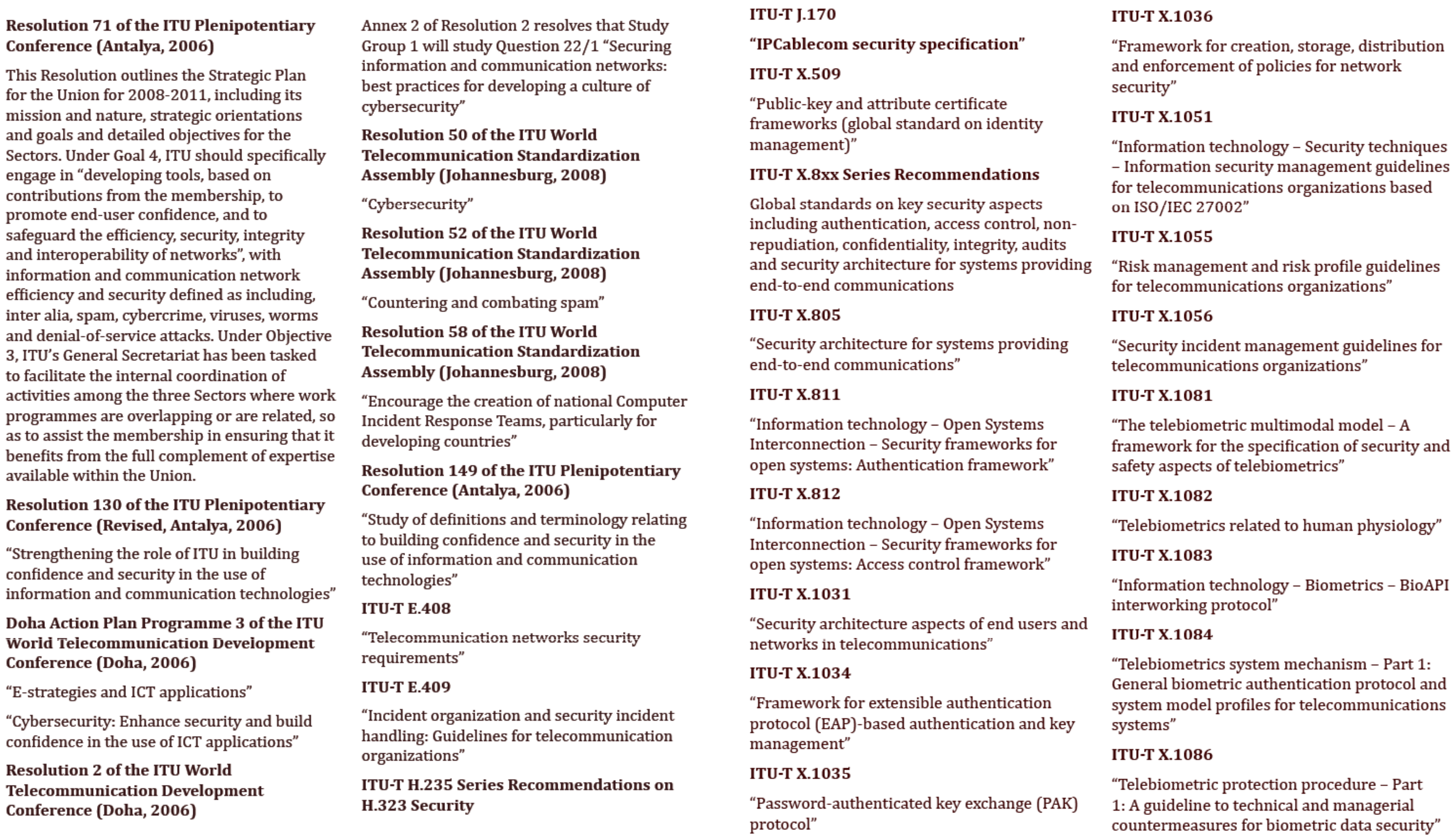
ITU-T X-SERIES RECOMMENDATIONS

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.

ITU Resolutions & Security Standards (1)



Resolution 71 of the ITU Plenipotentiary Conference (Antalya, 2006)

This Resolution outlines the Strategic Plan for the Union for 2008-2011, including its mission and nature, strategic orientations and goals and detailed objectives for the Sectors. Under Goal 4, ITU should specifically engage in "developing tools, based on contributions from the membership, to promote end-user confidence, and to safeguard the efficiency, security, integrity and interoperability of networks", with information and communication network efficiency and security defined as including, inter alia, spam, cybercrime, viruses, worms and denial-of-service attacks. Under Objective 3, ITU's General Secretariat has been tasked to facilitate the internal coordination of activities among the three Sectors where work programmes are overlapping or are related, so as to assist the membership in ensuring that it benefits from the full complement of expertise available within the Union.

Resolution 130 of the ITU Plenipotentiary Conference (Revised, Antalya, 2006)

"Strengthening the role of ITU in building confidence and security in the use of information and communication technologies"

Doha Action Plan Programme 3 of the ITU World Telecommunication Development Conference (Doha, 2006)

"E-strategies and ICT applications"

"Cybersecurity: Enhance security and build confidence in the use of ICT applications"

Resolution 2 of the ITU World Telecommunication Development Conference (Doha, 2006)

Annex 2 of Resolution 2 resolves that Study Group 1 will study Question 22/1 "Securing information and communication networks: best practices for developing a culture of cybersecurity"

Resolution 50 of the ITU World Telecommunication Standardization Assembly (Johannesburg, 2008)

"Cybersecurity"

Resolution 52 of the ITU World Telecommunication Standardization Assembly (Johannesburg, 2008)

"Countering and combating spam"

Resolution 58 of the ITU World Telecommunication Standardization Assembly (Johannesburg, 2008)

"Encourage the creation of national Computer Incident Response Teams, particularly for developing countries"

Resolution 149 of the ITU Plenipotentiary Conference (Antalya, 2006)

"Study of definitions and terminology relating to building confidence and security in the use of information and communication technologies"

ITU-T E.408

"Telecommunication networks security requirements"

ITU-T E.409

"Incident organization and security incident handling: Guidelines for telecommunication organizations"

ITU-T H.235 Series Recommendations on H.323 Security

ITU-T J.170

"IPCablecom security specification"

ITU-T X.509

"Public-key and attribute certificate frameworks (global standard on identity management)"

ITU-T X.8xx Series Recommendations

Global standards on key security aspects including authentication, access control, non-repudiation, confidentiality, integrity, audits and security architecture for systems providing end-to-end communications

ITU-T X.805

"Security architecture for systems providing end-to-end communications"

ITU-T X.811

"Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework"

ITU-T X.812

"Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework"

ITU-T X.1031

"Security architecture aspects of end users and networks in telecommunications"

ITU-T X.1034

"Framework for extensible authentication protocol (EAP)-based authentication and key management"

ITU-T X.1035

"Password-authenticated key exchange (PAK) protocol"

ITU-T X.1036

"Framework for creation, storage, distribution and enforcement of policies for network security"

ITU-T X.1051

"Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002"

ITU-T X.1055

"Risk management and risk profile guidelines for telecommunications organizations"

ITU-T X.1056

"Security incident management guidelines for telecommunications organizations"

ITU-T X.1081

"The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics"

ITU-T X.1082

"Telebiometrics related to human physiology"

ITU-T X.1083

"Information technology – Biometrics – BioAPI interworking protocol"

ITU-T X.1084

"Telebiometrics system mechanism – Part 1: General biometric authentication protocol and system model profiles for telecommunications systems"

ITU-T X.1086

"Telebiometric protection procedure – Part 1: A guideline to technical and managerial countermeasures for biometric data security"

ITU Resolutions & Security Standards (2)

ITU-T X.1088

"Telebiometrics digital key framework (TDK) – A framework for biometric digital key generation and protection"

ITU-T X.1089

"Telebiometrics authentication infrastructure (TAI) "

ITU-T X.1111

"Framework for security technologies for home network"

ITU-T X.1112

"Device certificate profile for the home network"

ITU-T X.1113

"Guideline on user authentication mechanism for home network services"

ITU-T X.1114

"Authorization framework for home network"

ITU-T X.1121

"Framework of security technologies for mobile end-to-end data communications"

ITU-T X.1122

"Guideline for implementing secure mobile systems based on PKI"

ITU-T X.1123

"Differentiated security service for secure mobile end-to-end data communication"

ITU-T X.1124

"Authentication architecture for mobile end-to-end data communication"

ITU-T X.1125

"Correlative Reacting System in mobile data communication"

ITU-T X.1141

"Security Assertion Markup Language (SAML 2.0)"

ITU-T X.1142

"Web services security – eXtensible Access Control Markup Language (XACML 2.0)"

ITU-T X.1143

"Security architecture for message security in mobile web services"

ITU-T X.1151

"Guideline on secure password-based authentication protocol with key exchange"

ITU-T X.1152

"Secure end-to-end data communication techniques using trusted third party services"

ITU-T X.1161

"Framework for secure peer-to-peer communications"

ITU-T X.1162

"Security architecture and operations for peer-to-peer network"

ITU-T X.1171

"Threats and requirements for protection of personally identifiable information in applications using tag-based identification"

ITU-T X.1191

"Functional requirements and architecture for IPTV security aspects"

ITU-T X.1205

"Overview of cybersecurity"

ITU-T X.1206

"A vendor-neutral framework for automatic notification of security related information and dissemination of updates"

ITU-T X.1207

"Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software"

ITU-T X.1231

"Technical strategies for countering spam"

ITU-T X.1240

"Technologies involved in countering email spam"

ITU-T X.1241

"Technical framework for countering email spam"

ITU-T X.1242

"Short message service (SMS) spam filtering system based on user-specified rules"

ITU-T X.1244

ITU-T "Overall aspects of countering spam in IP-based multimedia applications"

ITU-T X.1303

"Common alerting protocol (CAP 1.1)"

Resolution 45 of the ITU World Telecommunication Development Conference (Doha, 2006)

"Mechanisms for enhancing cooperation on cybersecurity, including combating spam"

Recommendation ITU-R M.1078

"Security principles for IMT-2000"

Recommendation ITU-R M.1223

"Evaluation of security mechanisms for IMT-2000"

Recommendation ITU-R M.1457

"Security mechanisms incorporated in IMT-2000"

Recommendation ITU-R M.1645

"Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000"

Recommendation ITU-R S.1250

"Network management architecture for digital satellite systems forming part of SDH transport networks in the fixed satellite service"

Recommendation ITU-R S.1711

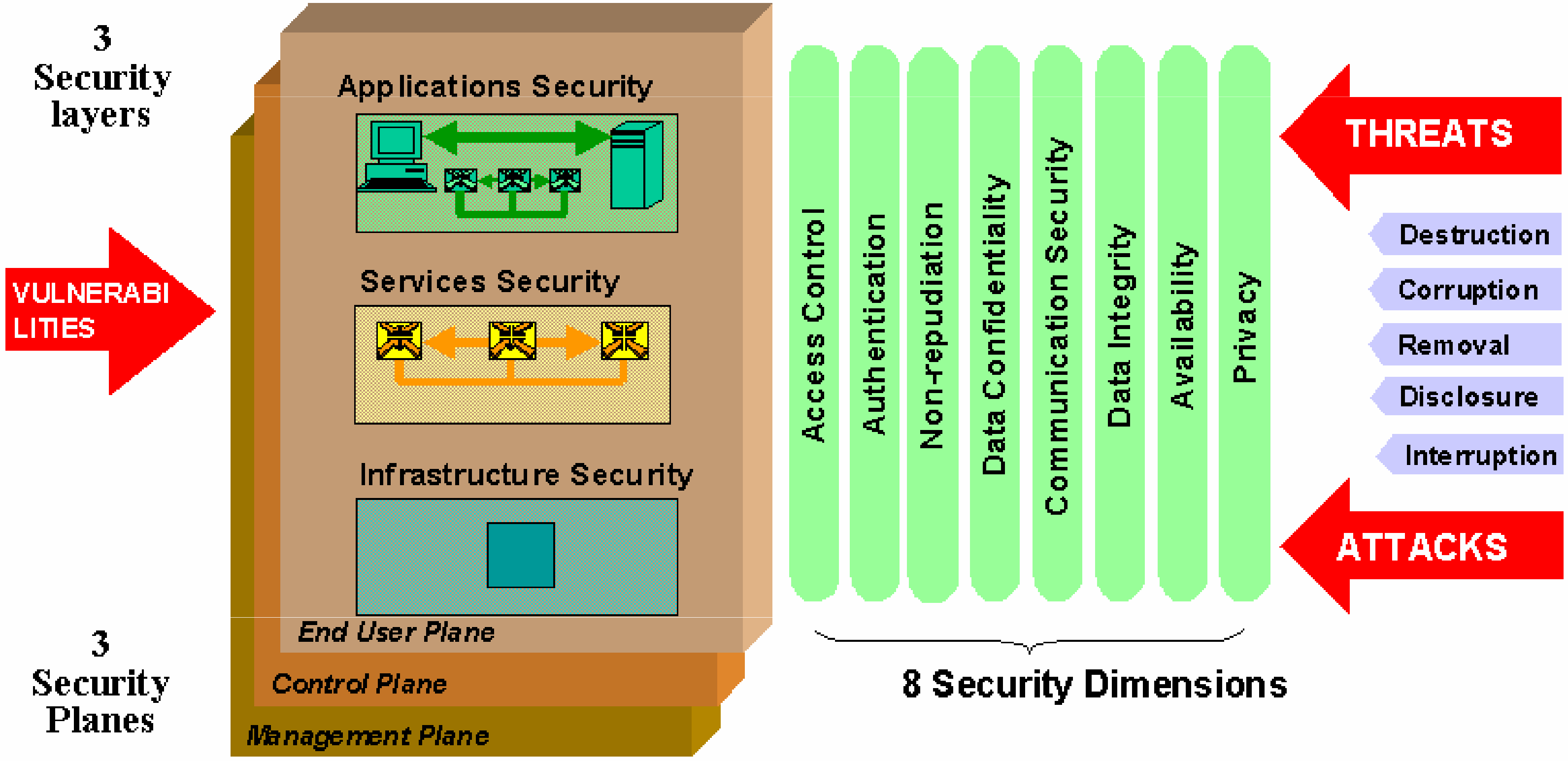
"Performance enhancements of transmission control protocol over satellite networks"

* Workshop Session 5 *

"Cybersecurity Continuity Planning, Standards and Architectures"

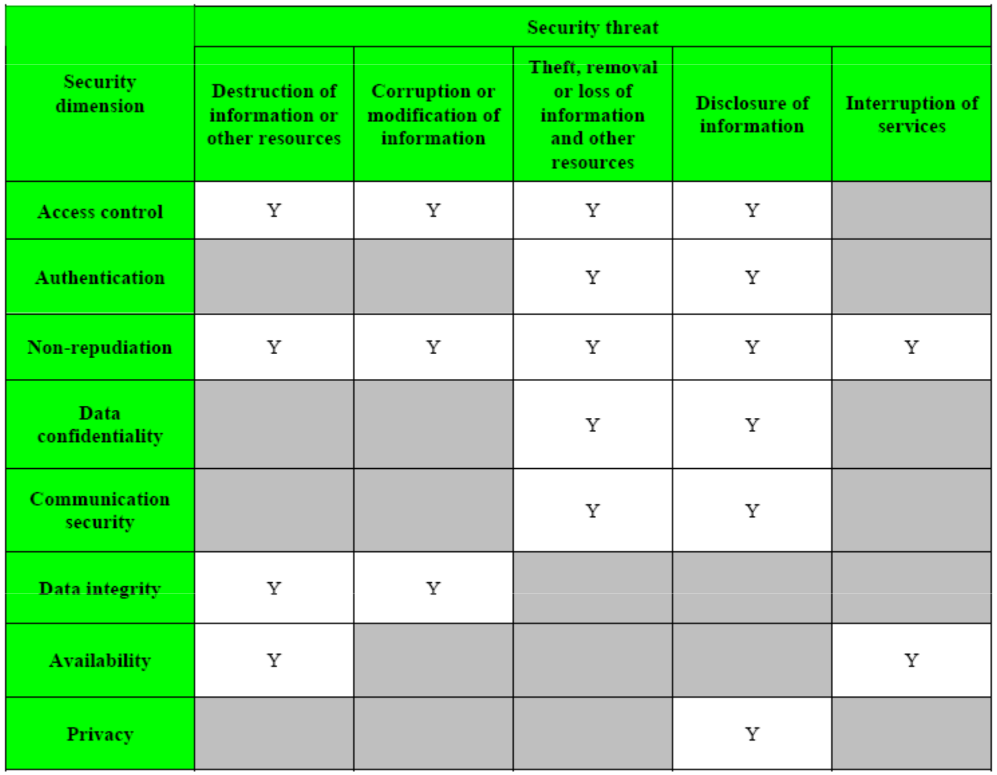
1 – International Standards	2 – ITU Security Standards	3 – ITU: X.805 Architecture
4 – ITU: X1205 CyberSecurity	5 – Others: ISO/IEC & NIST	6 – ISF: Info Security Forum
7 – Practical Implementation	8 – Cyber Continuity: BCP/DR	9 – Next Steps for Jamaica

ITU – X.805 Security Architecture



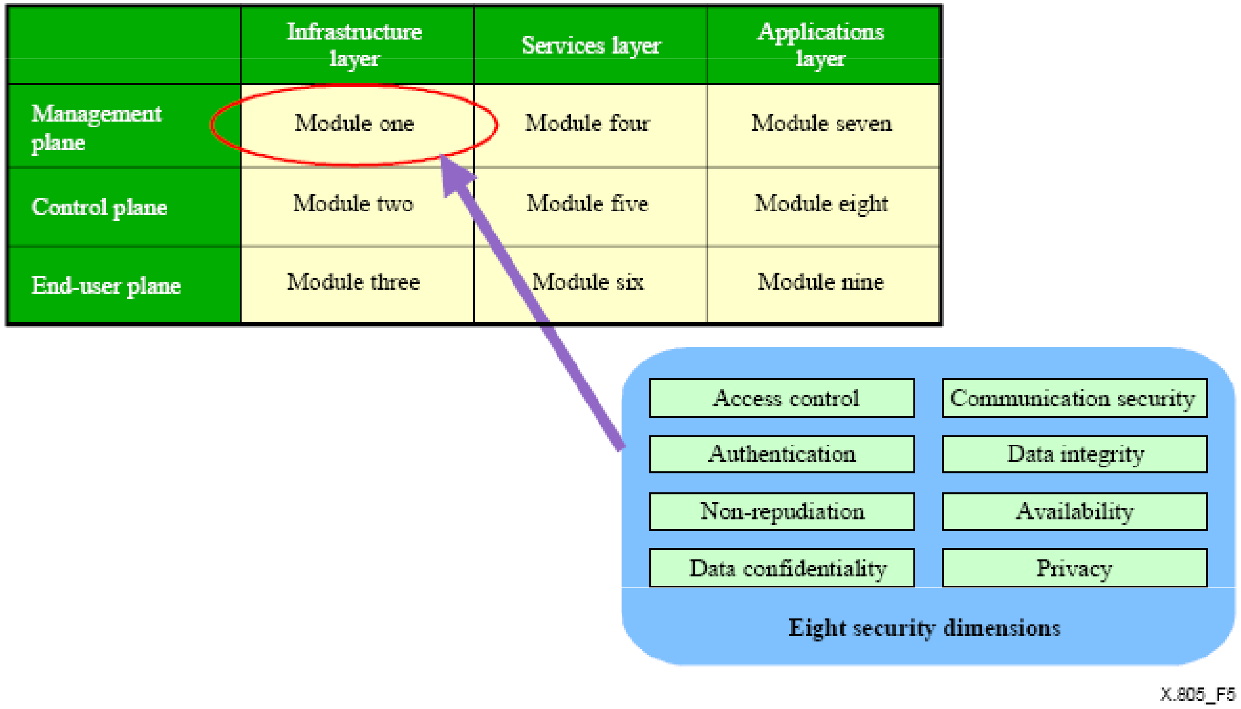
X.805 – Mapping Security Dimensions to Threats

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	

X.805 : 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

Access control	Communication security
Authentication	Data integrity
Non-repudiation	Availability
Data confidentiality	Privacy

Eight security dimensions

X.805_F5

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

X.805: Security Module 4

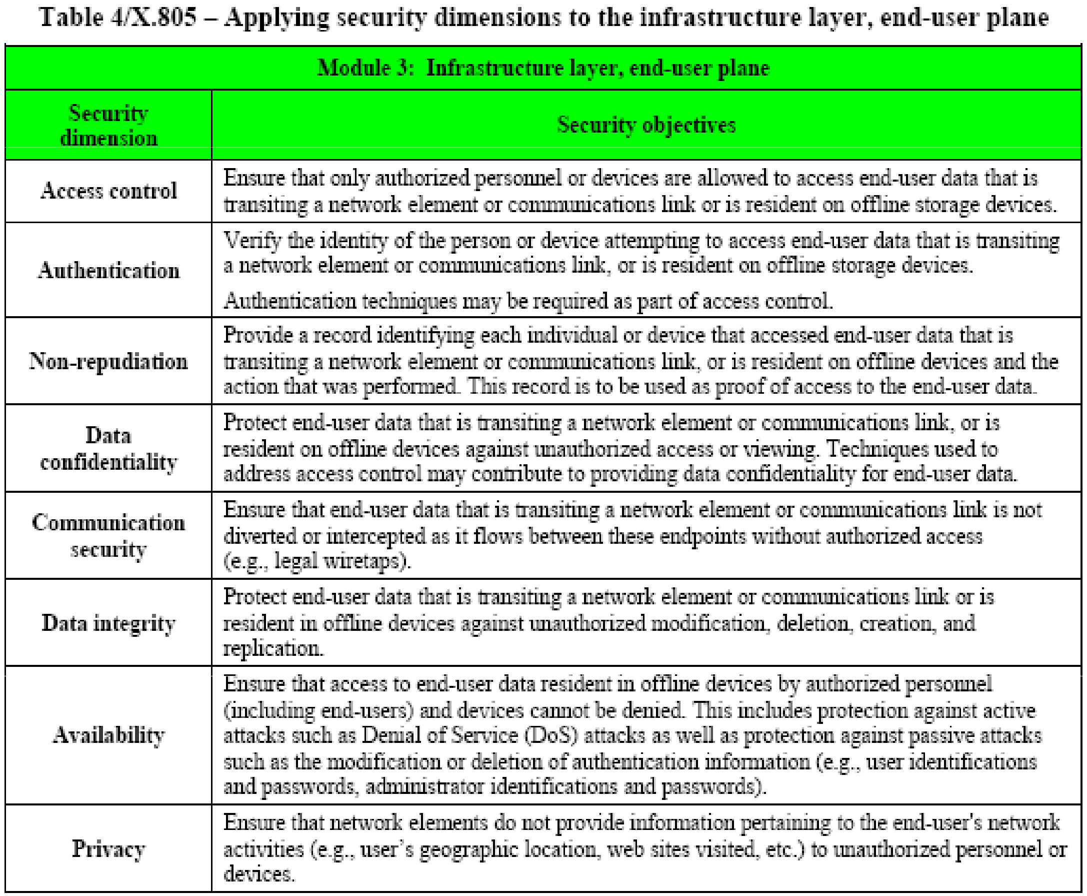
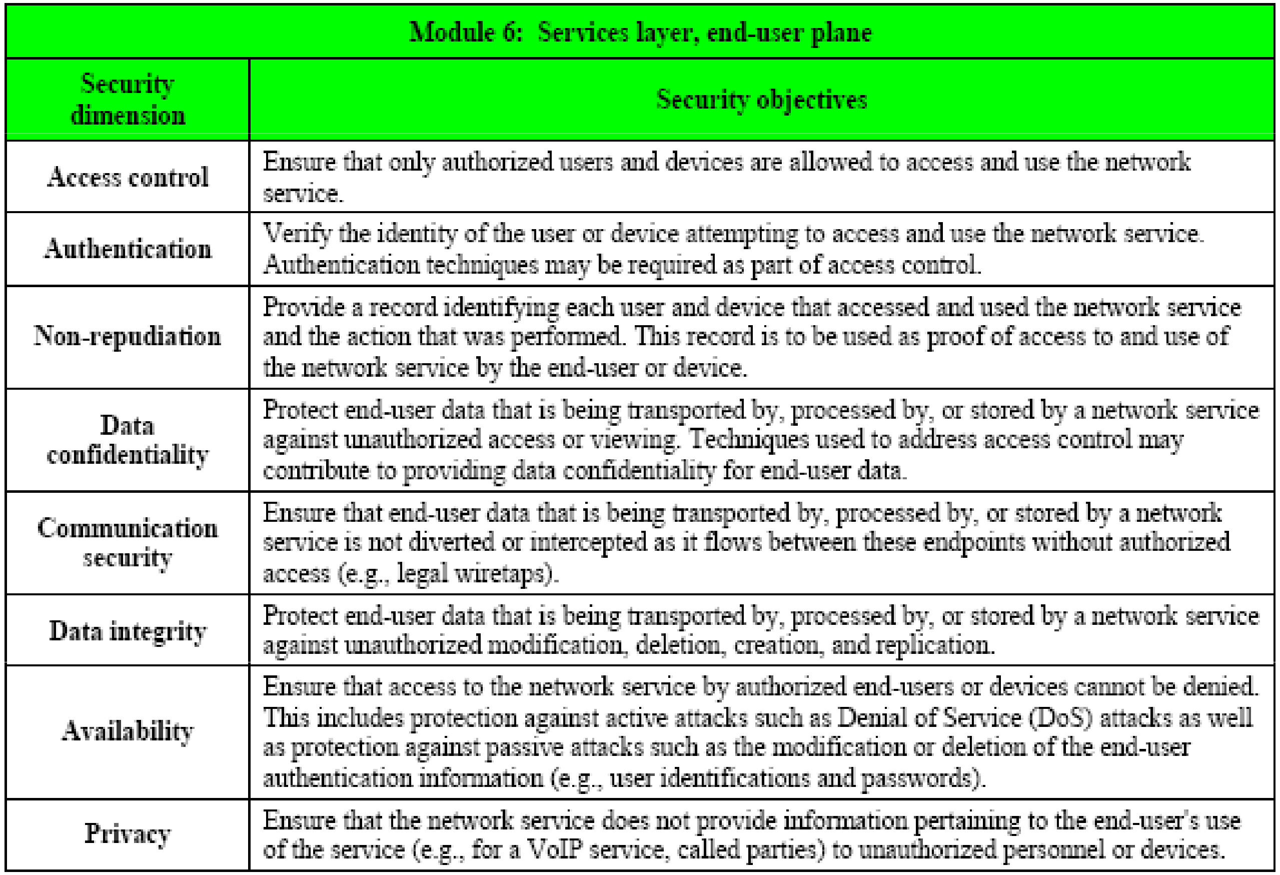


Table 4/X.805 – Applying security dimensions to the infrastructure layer, end-user plane

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.

X.805: Security Module 6

Table 7/X.805 – Applying security dimensions to the services layer, end-user plane



Module 6: Services layer, end-user plane	
Security dimension	Security objectives
Access control	Ensure that only authorized users and devices are allowed to access and use the network service.
Authentication	Verify the identity of the user or device attempting to access and use the network service. Authentication techniques may be required as part of access control.
Non-repudiation	Provide a record identifying each user and device that accessed and used the network service and the action that was performed. This record is to be used as proof of access to and use of the network service by the end-user or device.
Data confidentiality	Protect end-user data that is being transported by, processed by, or stored by a network service 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 being transported by, processed by, or stored by a network service 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 being transported by, processed by, or stored by a network service against unauthorized modification, deletion, creation, and replication.
Availability	Ensure that access to the network service by authorized end-users or 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 the end-user authentication information (e.g., user identifications and passwords).
Privacy	Ensure that the network service does not provide information pertaining to the end-user's use of the service (e.g., for a VoIP service, called parties) to unauthorized personnel or devices.

X.805: Security Module 8

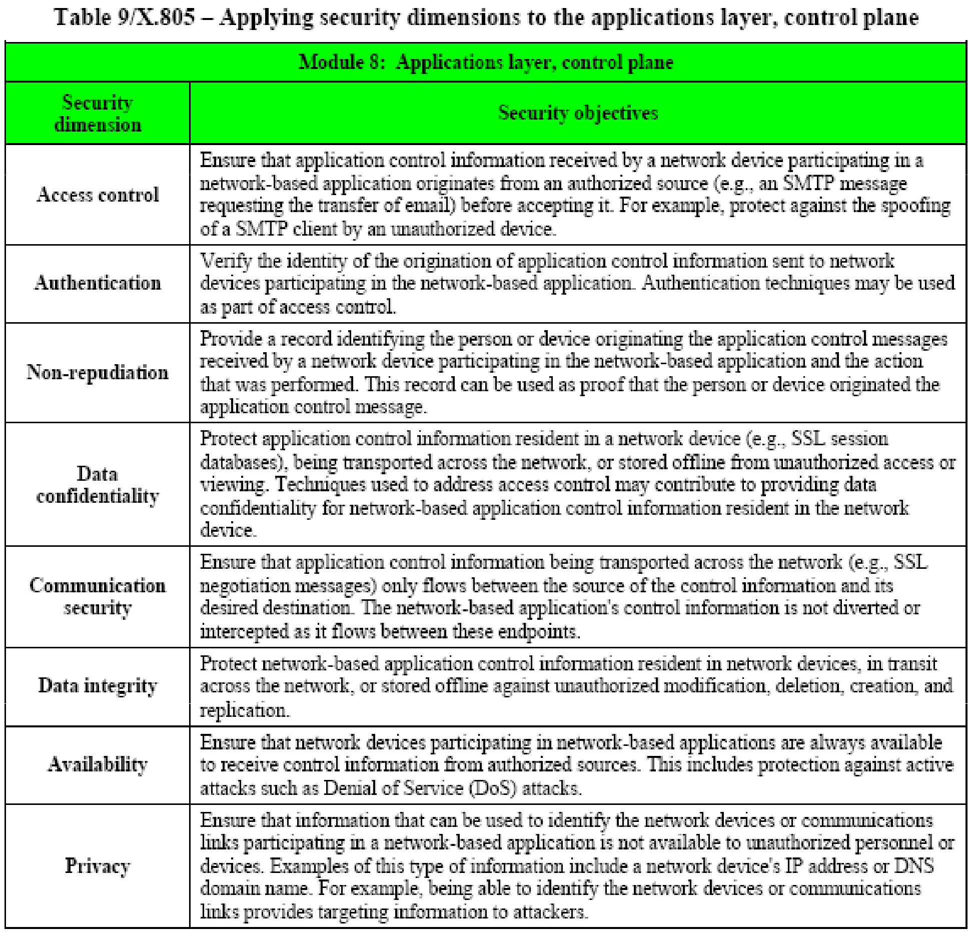
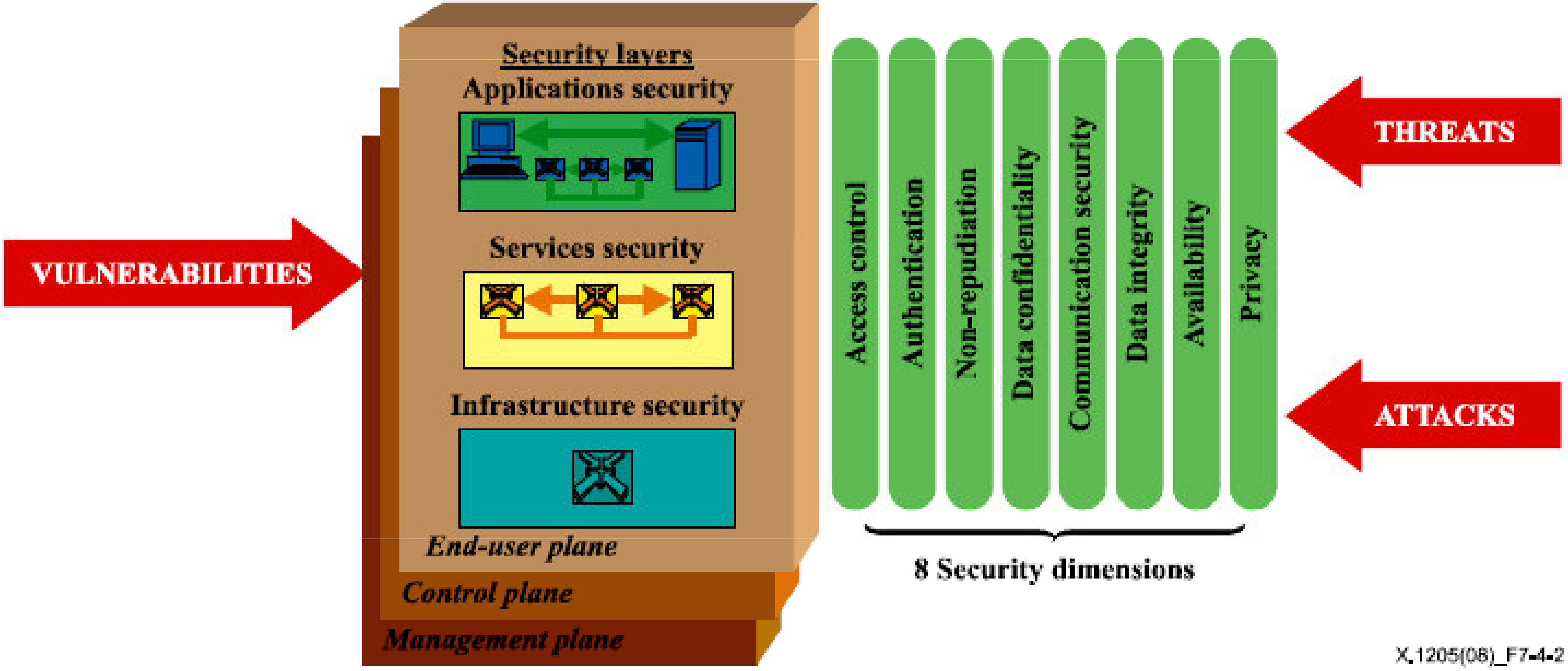


Table 9/X.805 – Applying security dimensions to the applications layer, control plane

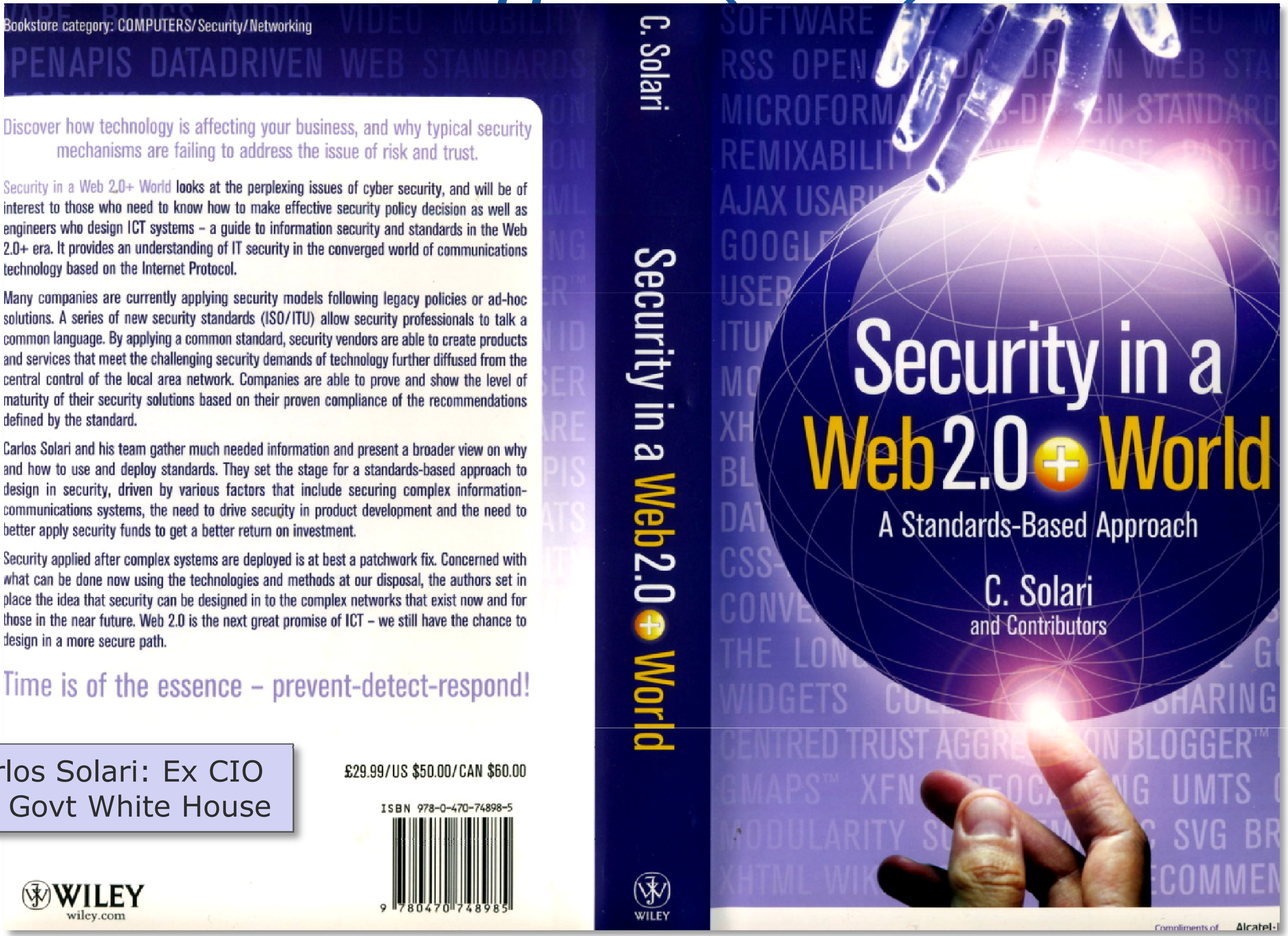
Module 8: Applications layer, control plane	
Security dimension	**Security objectives**
Access control	Ensure that application control information received by a network device participating in a network-based application originates from an authorized source (e.g., an SMTP message requesting the transfer of email) before accepting it. For example, protect against the spoofing of a SMTP client by an unauthorized device.
Authentication	Verify the identity of the origination of application control information sent to network devices participating in the network-based application. Authentication techniques may be used as part of access control.
Non-repudiation	Provide a record identifying the person or device originating the application control messages received by a network device participating in the network-based application and the action that was performed. This record can be used as proof that the person or device originated the application control message.
Data confidentiality	Protect application control information resident in a network device (e.g., SSL session databases), being transported across the network, or stored offline from unauthorized access or viewing. Techniques used to address access control may contribute to providing data confidentiality for network-based application control information resident in the network device.
Communication security	Ensure that application control information being transported across the network (e.g., SSL negotiation messages) only flows between the source of the control information and its desired destination. The network-based application's control information is not diverted or intercepted as it flows between these endpoints.
Data integrity	Protect network-based application control information resident in network devices, in transit across the network, or stored offline against unauthorized modification, deletion, creation, and replication.
Availability	Ensure that network devices participating in network-based applications are always available to receive control information from authorized sources. This includes protection against active attacks such as Denial of Service (DoS) attacks.
Privacy	Ensure that information that can be used to identify the network devices or communications links participating in a network-based application is not available to unauthorized personnel or devices. Examples of this type of information include a network device's IP address or DNS domain name. For example, being able to identify the network devices or communications links provides targeting information to attackers.

Security Planes & Network Activities



Recommended Book: Security in a Web2.0 World –

- *A Standards Based Approach(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!

£29.99/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 Web2.0+ World

A Standards-Based Approach

C. Solari
and Contributors

Compliments of Alcatel-

Carlos Solari: Ex CIO
US Govt White House

University of Technology, Jamaica

International Telecommunication Union

Committed to connecting the world

* Workshop Session 5 *

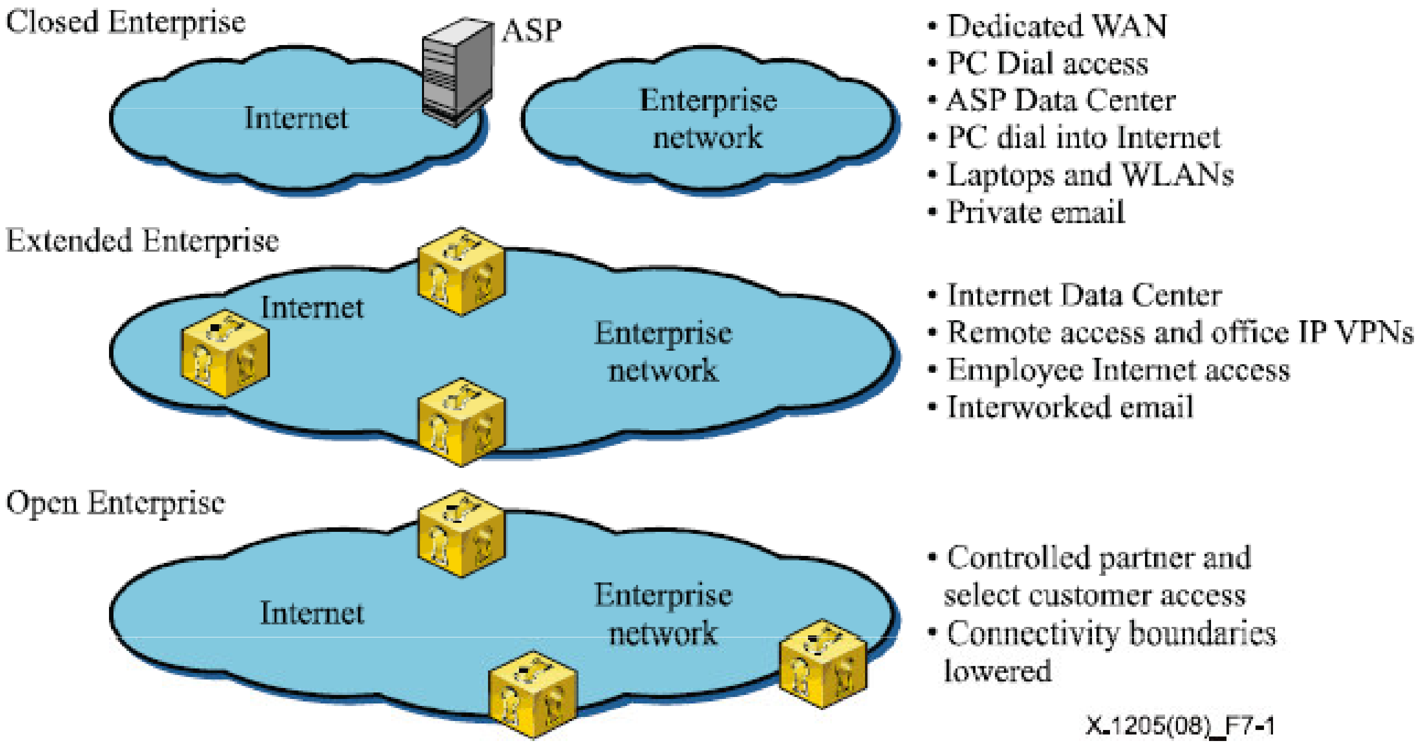
"Cybersecurity Continuity Planning, Standards and Architectures"

1 – International Standards	2 – ITU Security Standards	3 – ITU: X.805 Architecture
4 – ITU: X1205 CyberSecurity	5 – Others: ISO/IEC & NIST	6 – ISF: Info Security Forum
7 – Practical Implementation	8 – Cyber Continuity: BCP/DR	9 – Next Steps for Jamaica

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*

Typical Enterprise Networks



- Dedicated WAN
- PC Dial access
- ASP Data Center
- PC dial into Internet
- Laptops and WLANs
- Private email

- Internet Data Center
- Remote access and office IP VPNs
- Employee Internet access
- Interworked email

- Controlled partner and select customer access
- Connectivity boundaries lowered

X.1205(08)_F7-1

Secure Authentication and Authorization Reference Model

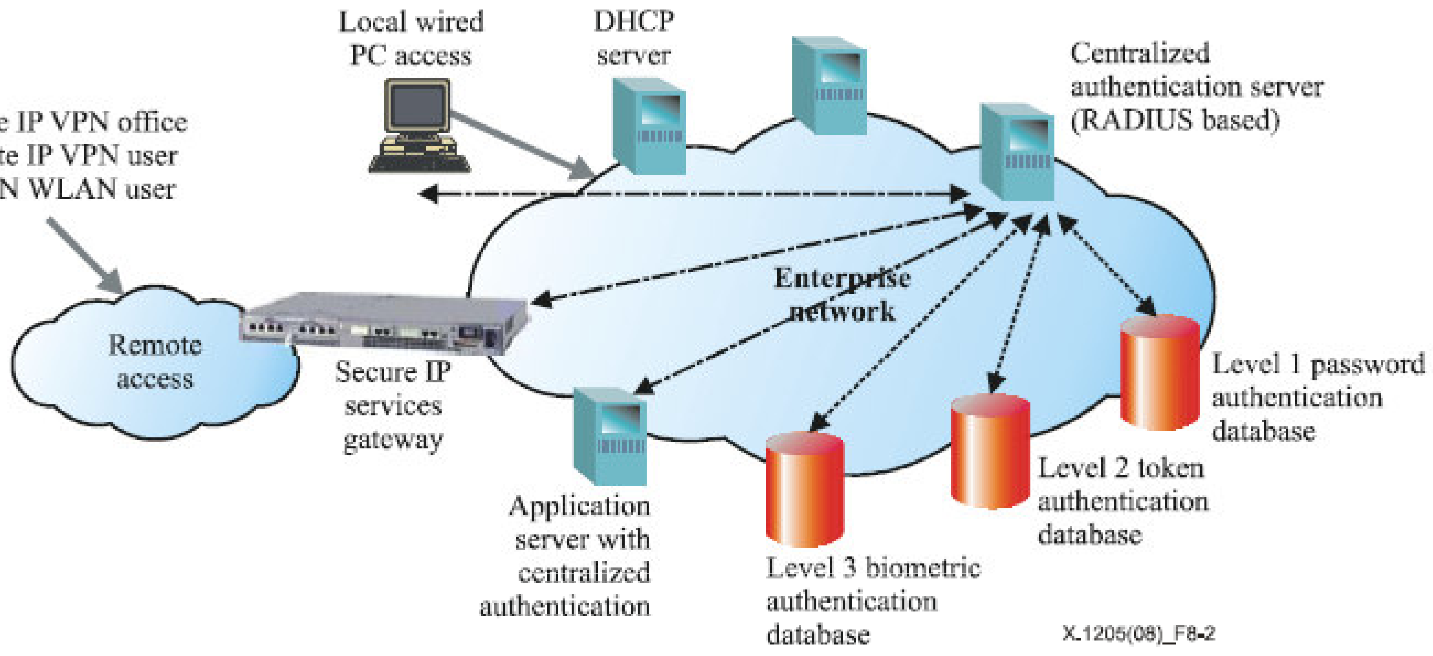
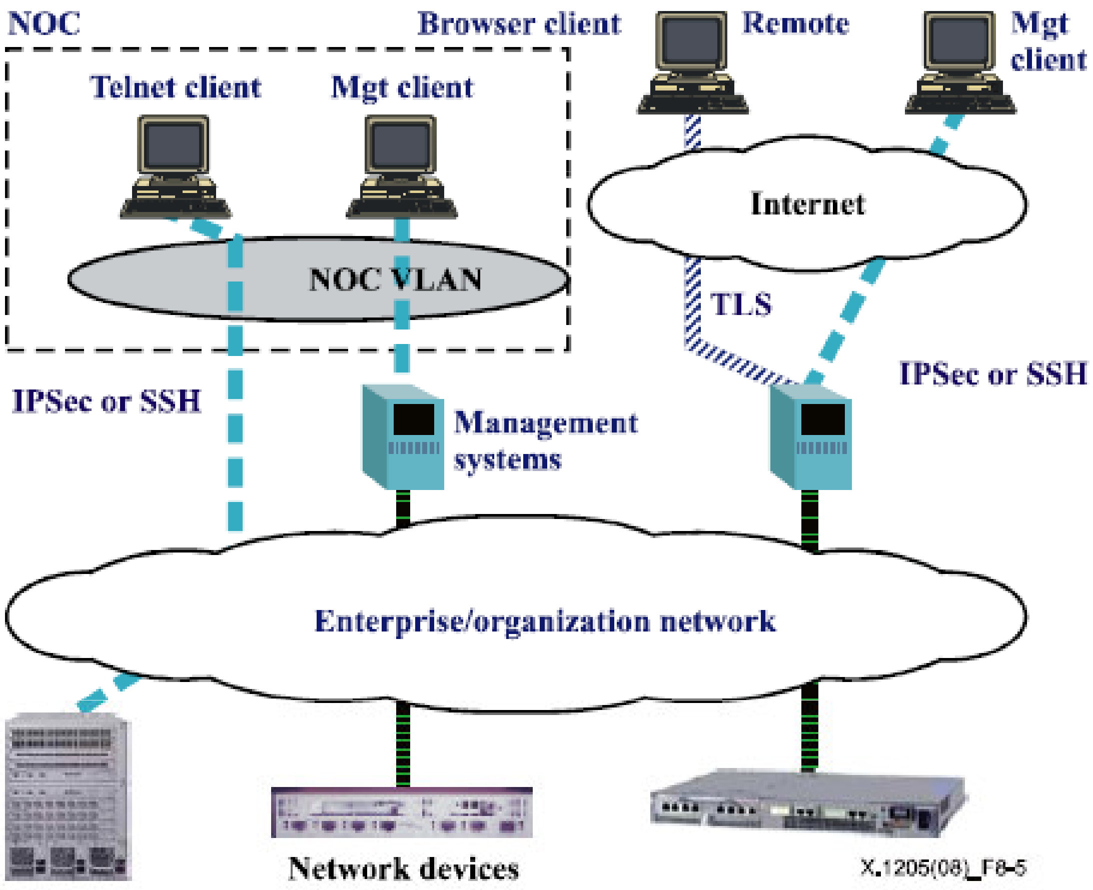
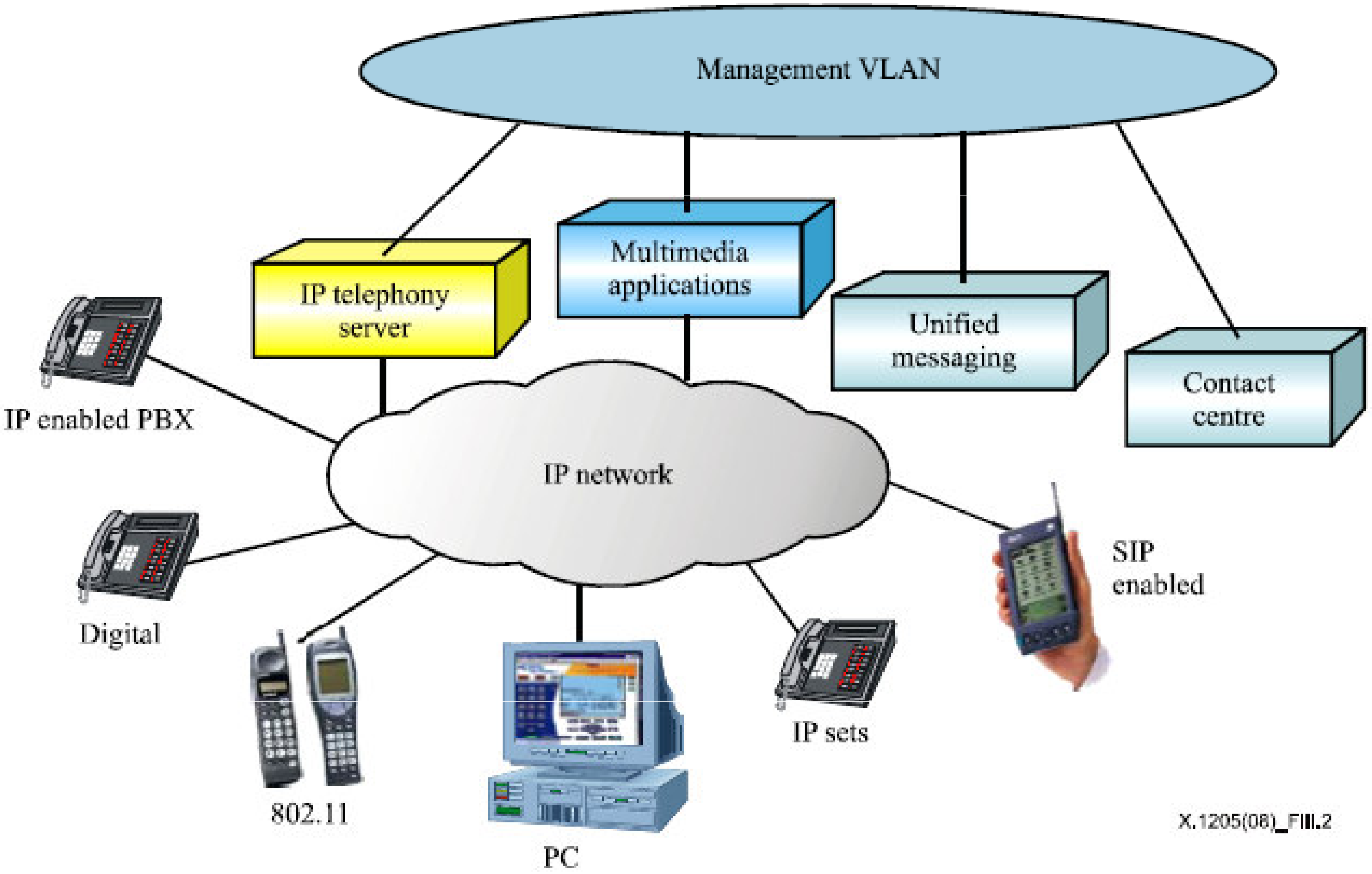


Figure 8-2 – Secure authentication and authorization reference model

Reference Model for Securing Management



Securing VoIP – IP Telephony – X.1205



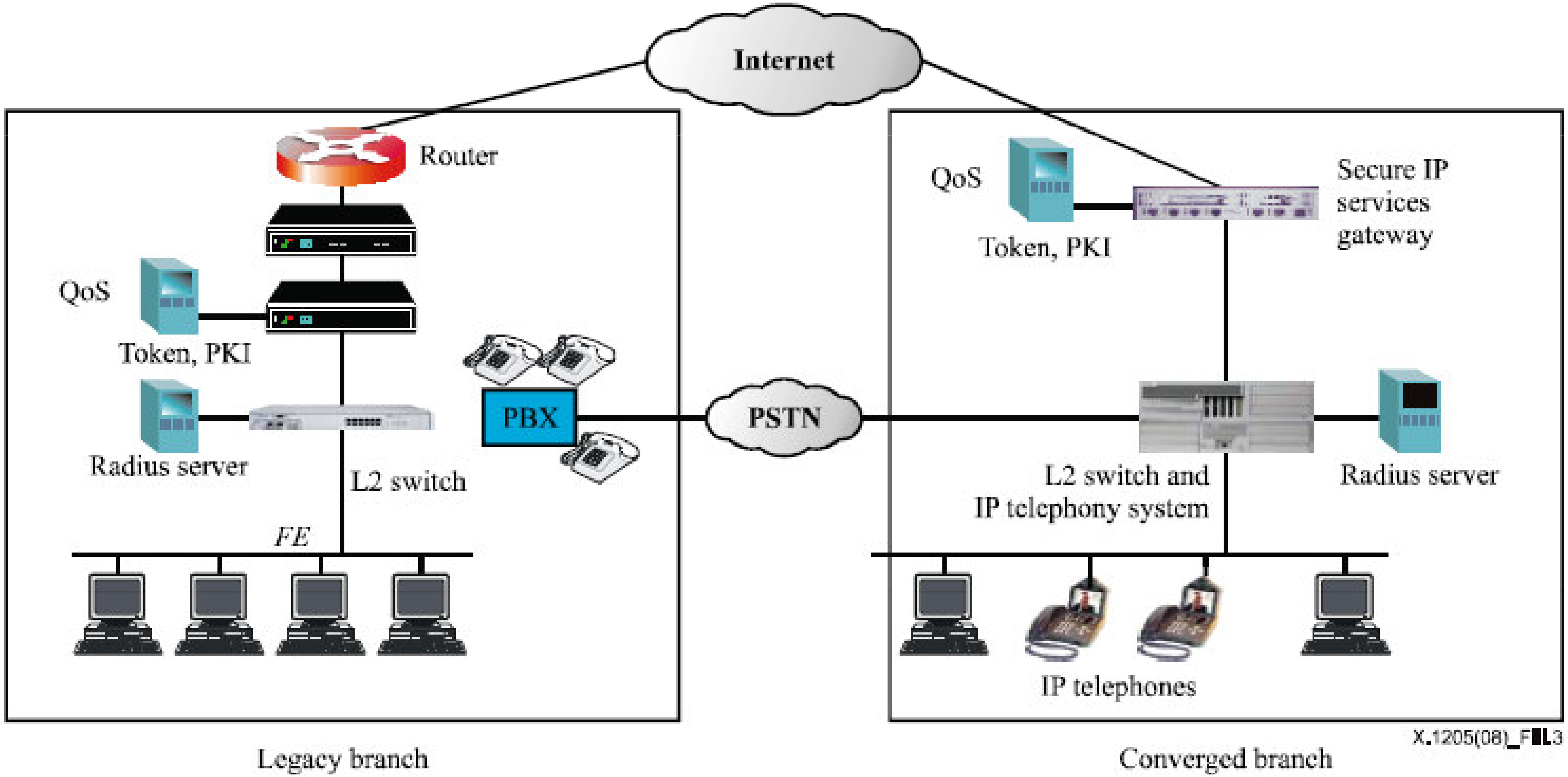
Cyber Risks for IP Telephony

- IP telephony systems can be subjected to a number of cyber attacks. For example:

- *Router:* Attacks on the router can bring down both voice and data services in an organization;
- *DDoS:* Denial of service can overload an IP telephony communications server or client;
- *Ping:* Ping of death can disrupt VoIP operations by sending multiple pings to VoIP devices;
- *Scanning*: Port scanning can find vulnerabilities in VoIP clients and servers;
- *Sniffing:* acket sniffing can record and/or intercept conversations;
- *Spoofing:* IP spoofing can misrepresent the source or destination of the media stream;
- *Malware:* Viruses, worms, Trojan horses, and time-triggered bots can attack servers and clients.

……..In summary, digital voice over IP is susceptible to practically all the same vulnerabilities, threats and risks as other forms of digital data communications. Hence all VoIP systems, clients, servers and comms links should be fully secured in the same manner as all other ICT applications.

Securing Remote Offices



Generic Wi-Fi Office Network

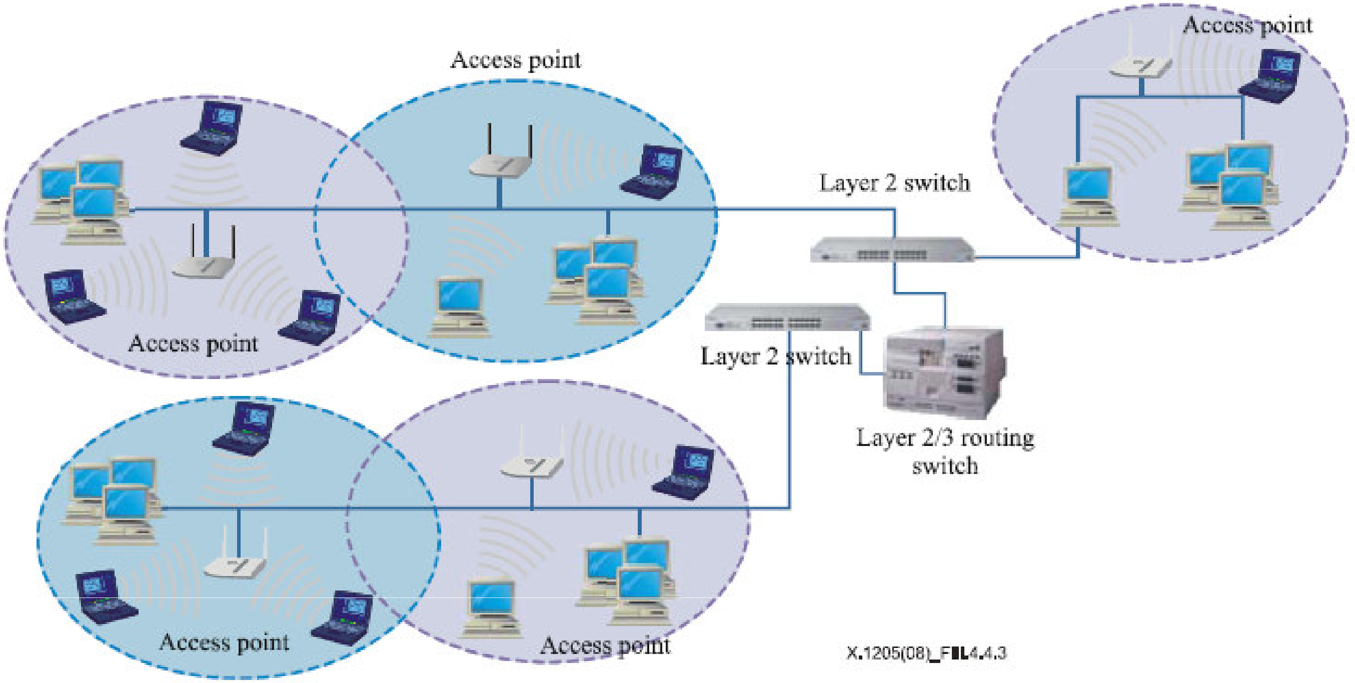
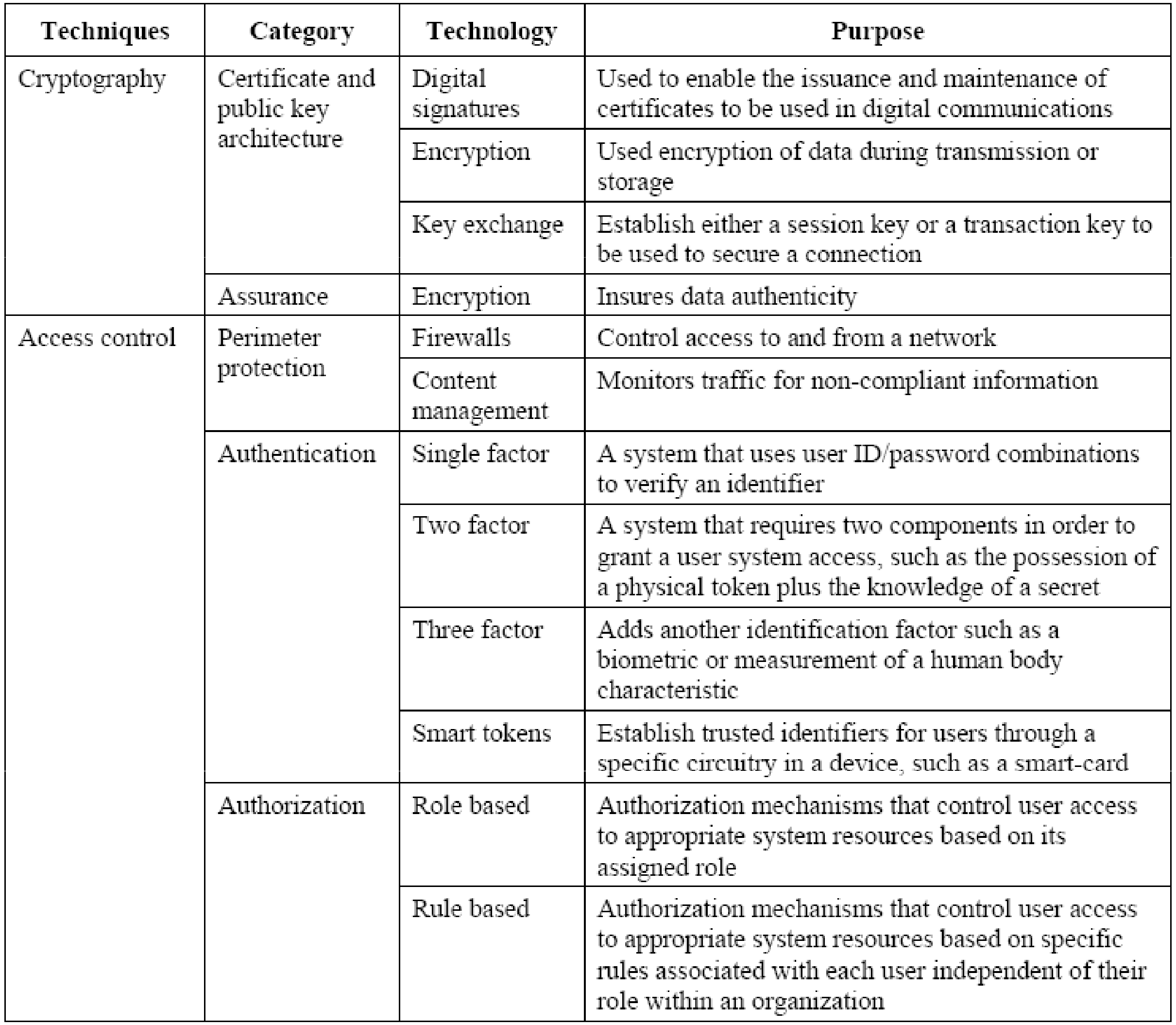


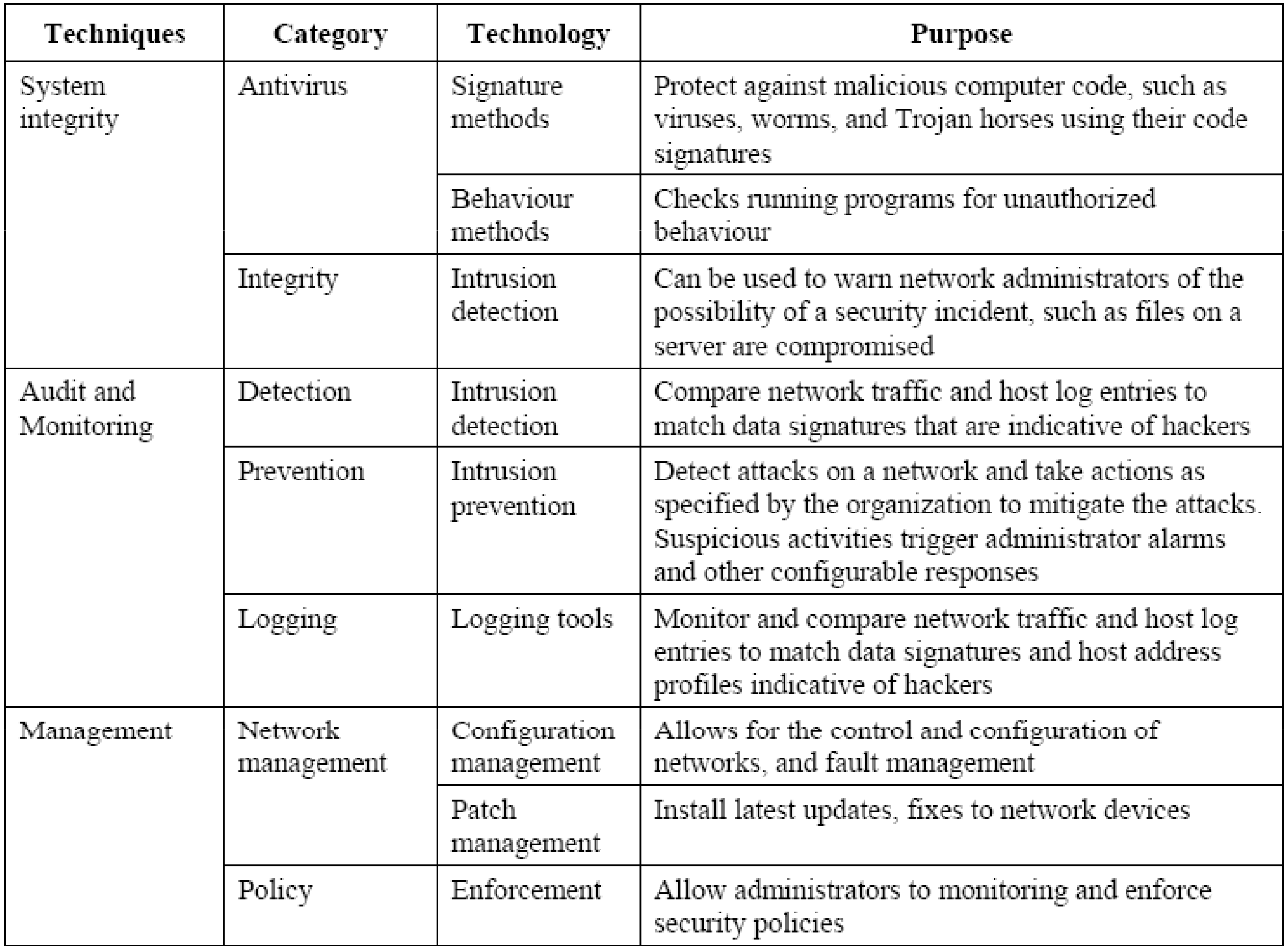
Figure III.4.4.3 – Generic WLAN IEEE 802.11 APs with a common SSID

X.1205 Cybersecurity Technologies (1)



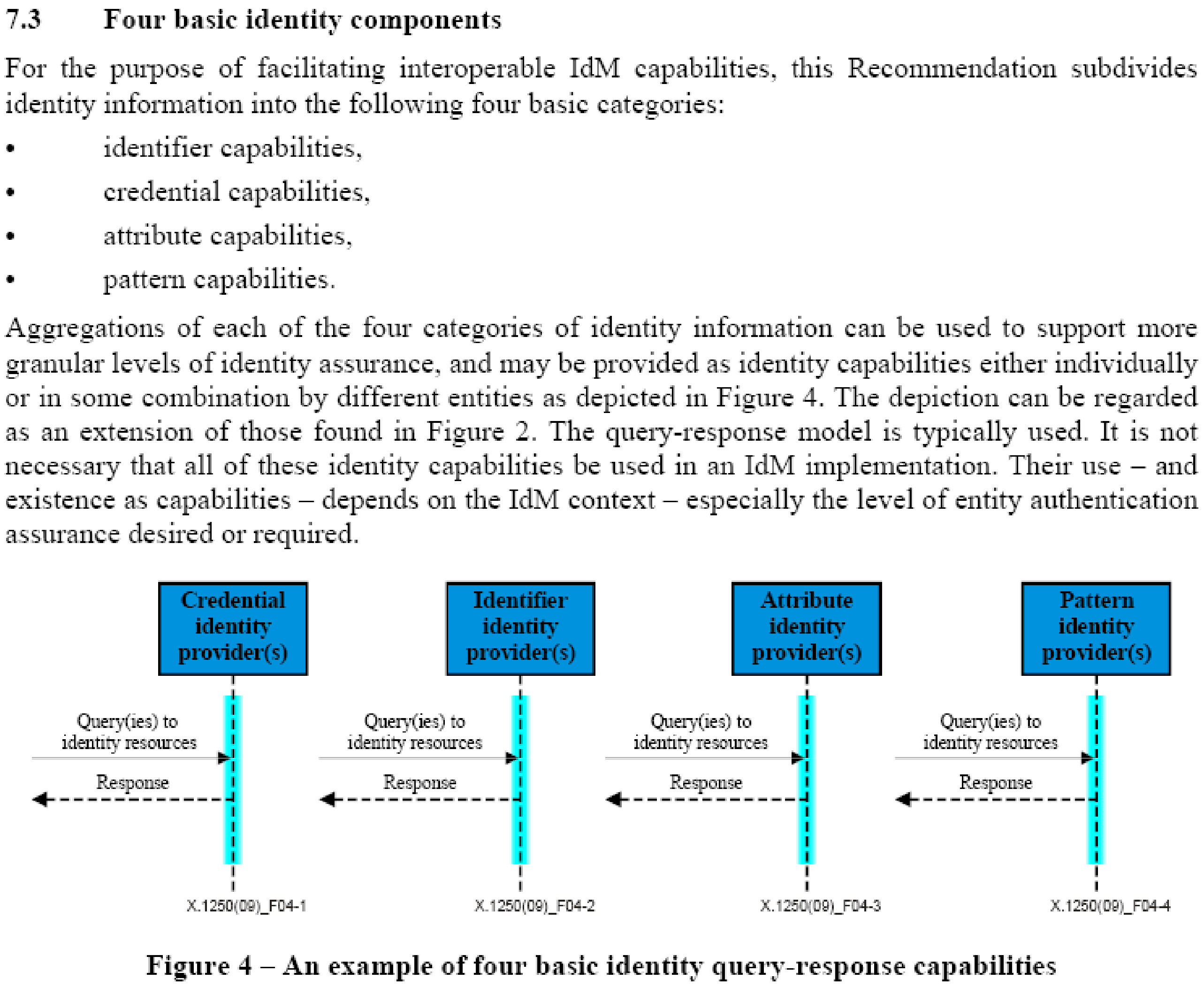
Techniques	Category	Technology	Purpose
Cryptography	Certificate and public key architecture	Digital signatures	Used to enable the issuance and maintenance of certificates to be used in digital communications
		Encryption	Used encryption of data during transmission or storage
		Key exchange	Establish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

Basic Categories for Identity Management – X.1250



7.3 Four basic identity components

For the purpose of facilitating interoperable IdM capabilities, this Recommendation subdivides identity information into the following four basic categories:

- identifier capabilities,
- credential capabilities,
- attribute capabilities,
- pattern capabilities.

Aggregations of each of the four categories of identity information can be used to support more granular levels of identity assurance, and may be provided as identity capabilities either individually or in some combination by different entities as depicted in Figure 4. The depiction can be regarded as an extension of those found in Figure 2. The query-response model is typically used. It is not necessary that all of these identity capabilities be used in an IdM implementation. Their use – and existence as capabilities – depends on the IdM context – especially the level of entity authentication assurance desired or required.

Credential identity provider(s)
Query(ies) to identity resources
Response
X.1250(09)_F04-1
Identifier identity provider(s)
Query(ies) to identity resources
Response
X.1250(09)_F04-2
Attribute identity provider(s)
Query(ies) to identity resources
Response
X.1250(09)_F04-3
Pattern identity provider(s)
Query(ies) to identity resources
Response
X.1250(09)_F04-4

Figure 4 – An example of four basic identity query-response capabilities

Identity Management (IdM) is required at all Network Levels

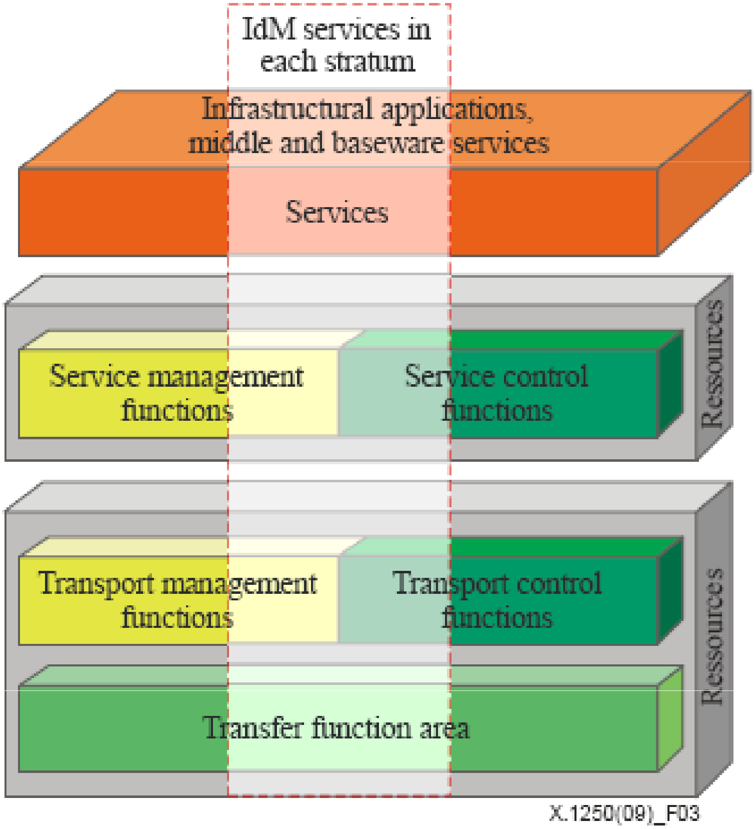

IdM services in each stratum
Infrastructural applications, middle and baseware services
Services
Service management functions
Service control functions
Ressources
Transport management functions
Transport control functions
Transfer function area
Ressources
X.1250(09)_F03

Figure 3 – Scope of identity management network strata interoperability

Identity Management Models: ITU-T X.1250

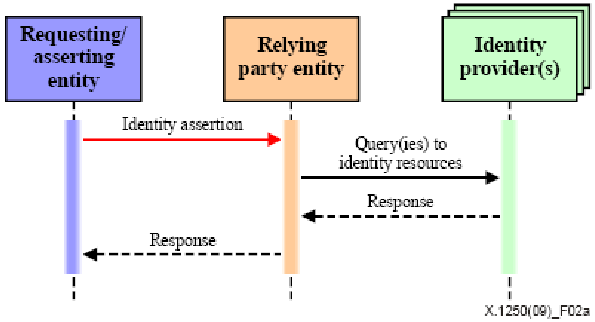
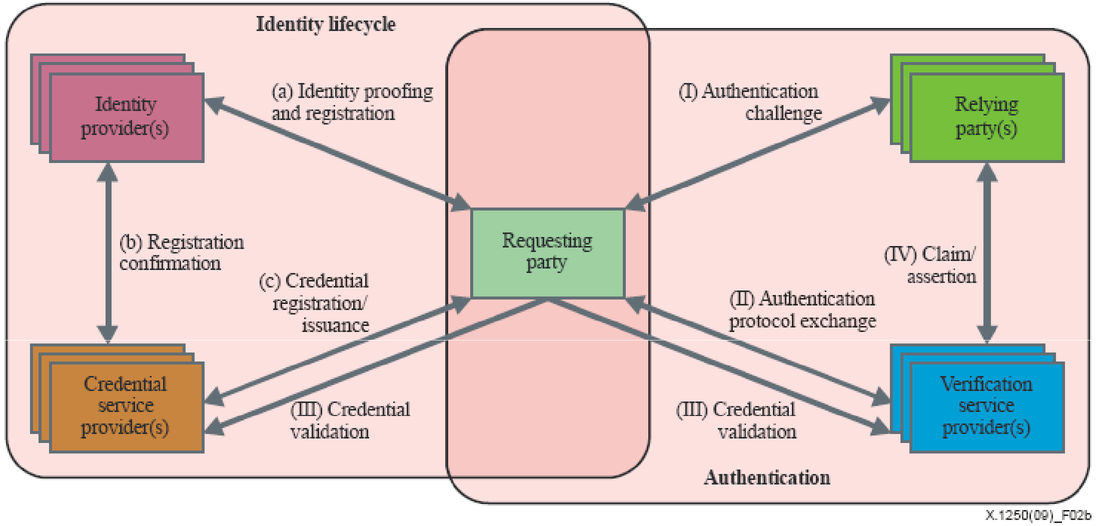


Figure 2a – An example of a three-party identity management model

Another identity management model that provides the requesting party with more control of the identity relationships is depicted in Figure 2b.



Identity lifecycle
Identity provider(s)
(a) Identity proofing and registration
(I) Authentication challenge
Relying party(s)
(b) Registration confirmation
Requesting party
(IV) Claim/ assertion
(c) Credential registration/ issuance
(II) Authentication protocol exchange
Credential service provider(s)
(III) Credential validation
(III) Credential validation
Verification service provider(s)
Authentication
X.1250(09)_F02b

Figure 2b – An example of a user-centric five-party identity management model

Identity Management Model

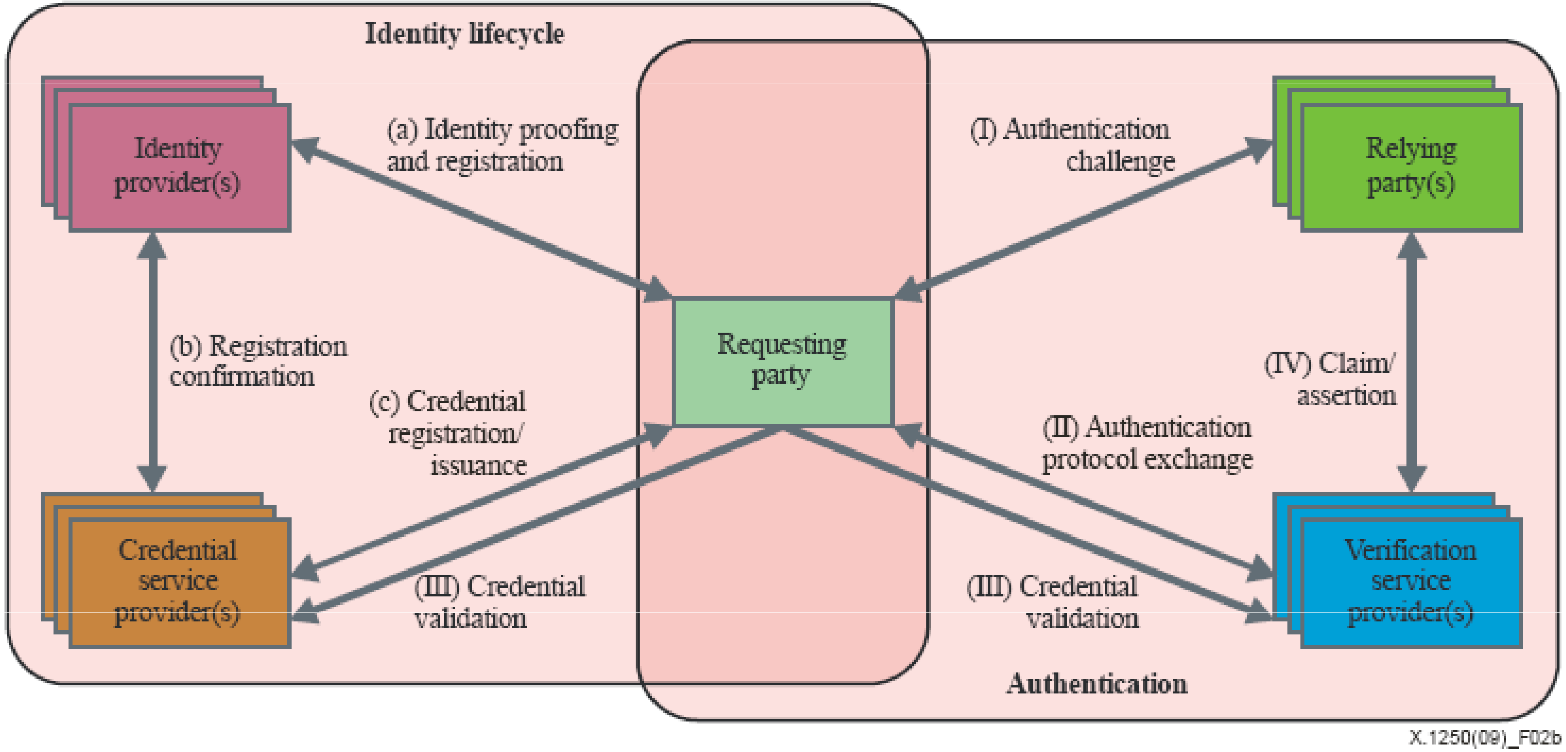
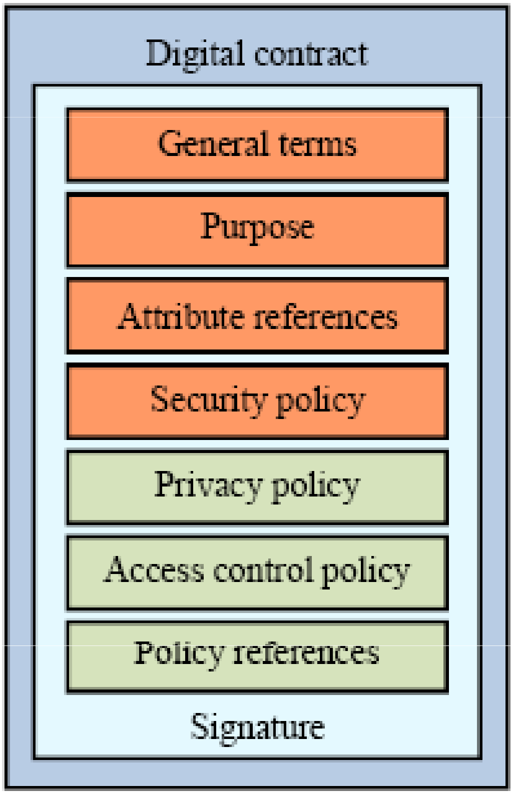

Identity lifecycle
Identity provider(s)
(a) Identity proofing and registration
(I) Authentication challenge
Relying party(s)
(b) Registration confirmation
Requesting party
(IV) Claim/ assertion
(c) Credential registration/ issuance
(II) Authentication protocol exchange
Credential service provider(s)
Verification service provider(s)
(III) Credential validation
(III) Credential validation
Authentication
X.1250(09)_F02b

Figure 2b – An example of a user-centric five-party identity management model

X.1251 - Generic Structure for a Digital Contract



X.1251(09)_F02

Conceptual Model for Digital Identity Interchange: X.1251

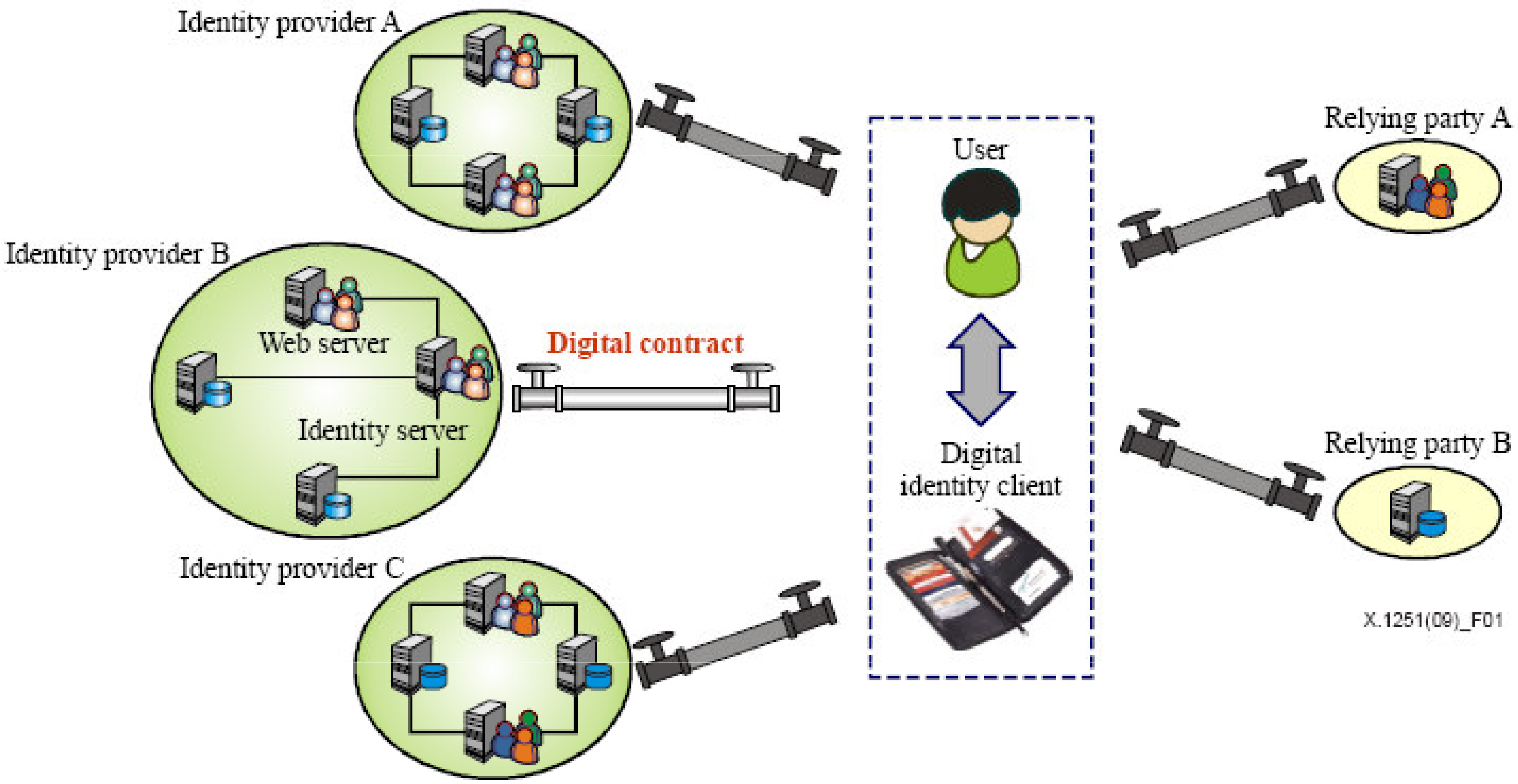
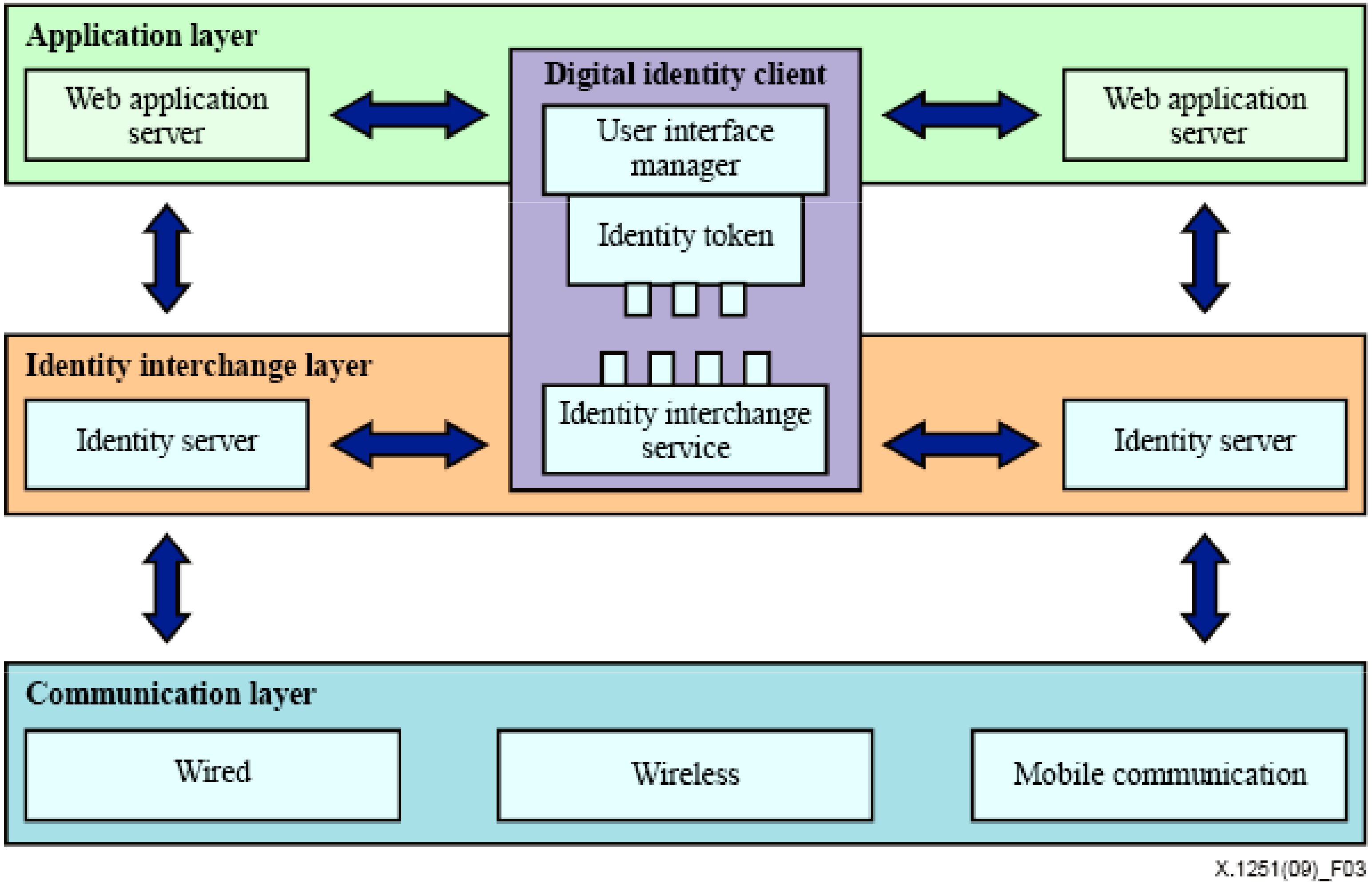
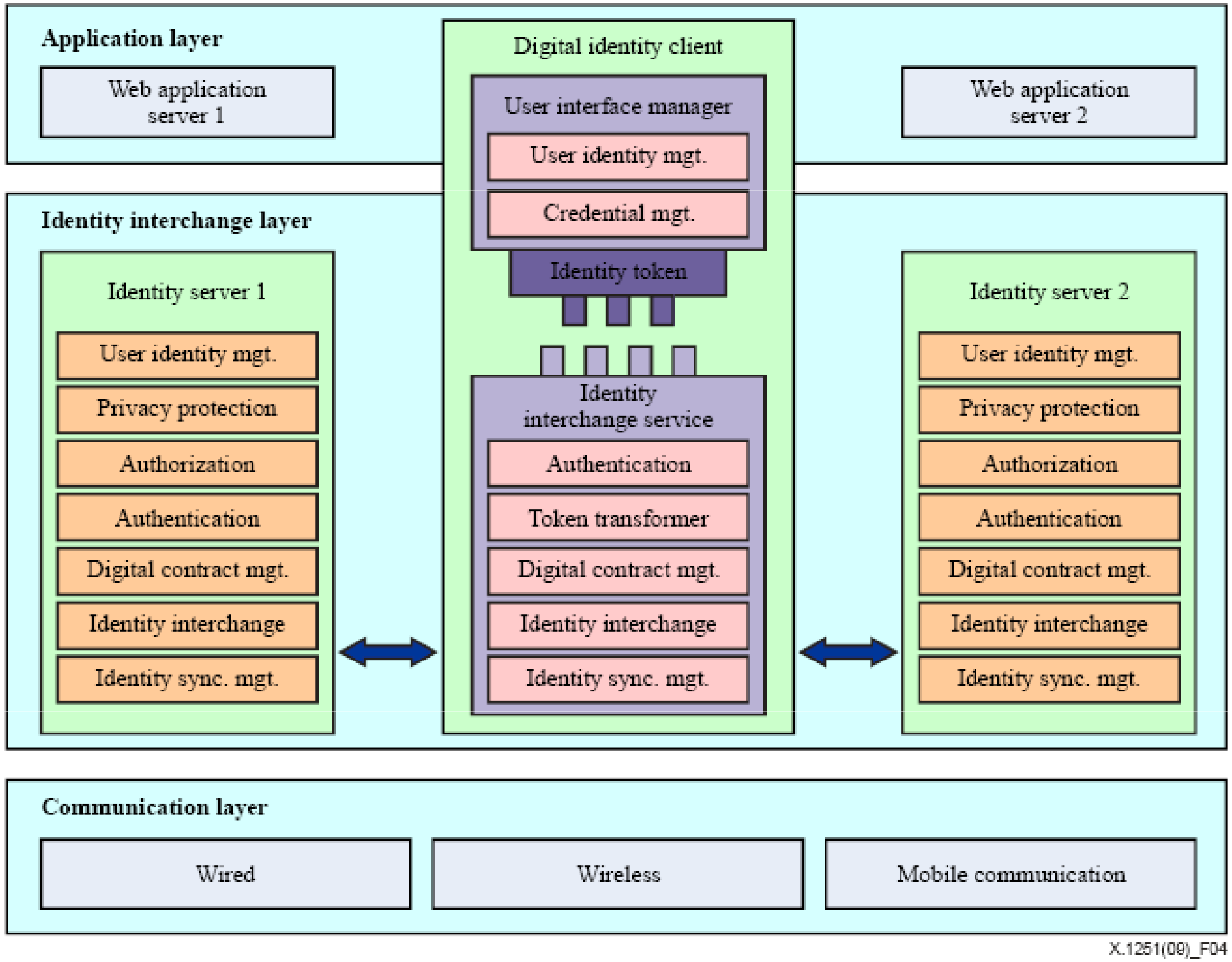


Figure 1 – The conceptual model for digital identity interchange

Identity Interchange Layer- X.1251



Digital Identity Interchange Framework – X.1251

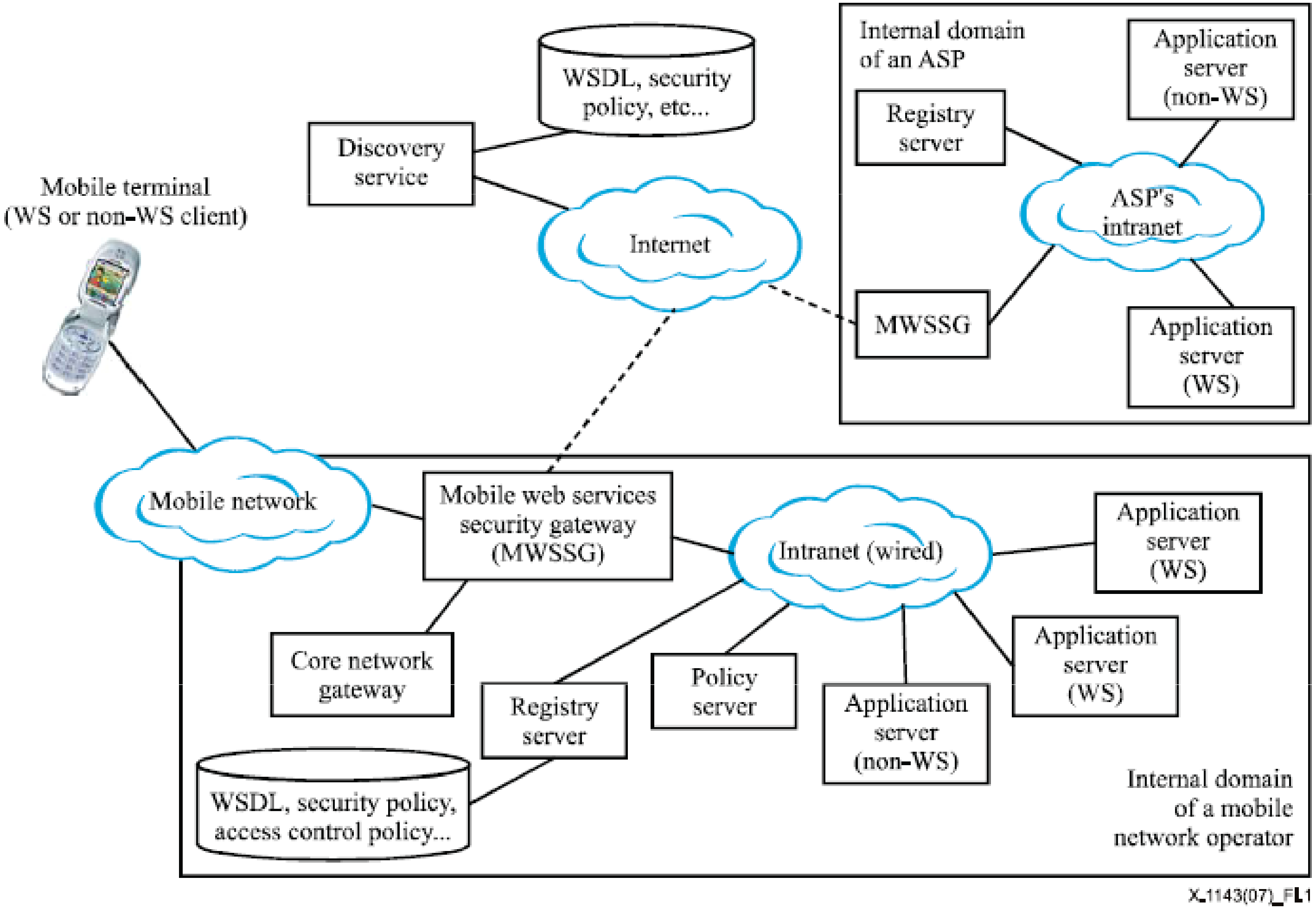


ITU X.1100 Security Standards Series

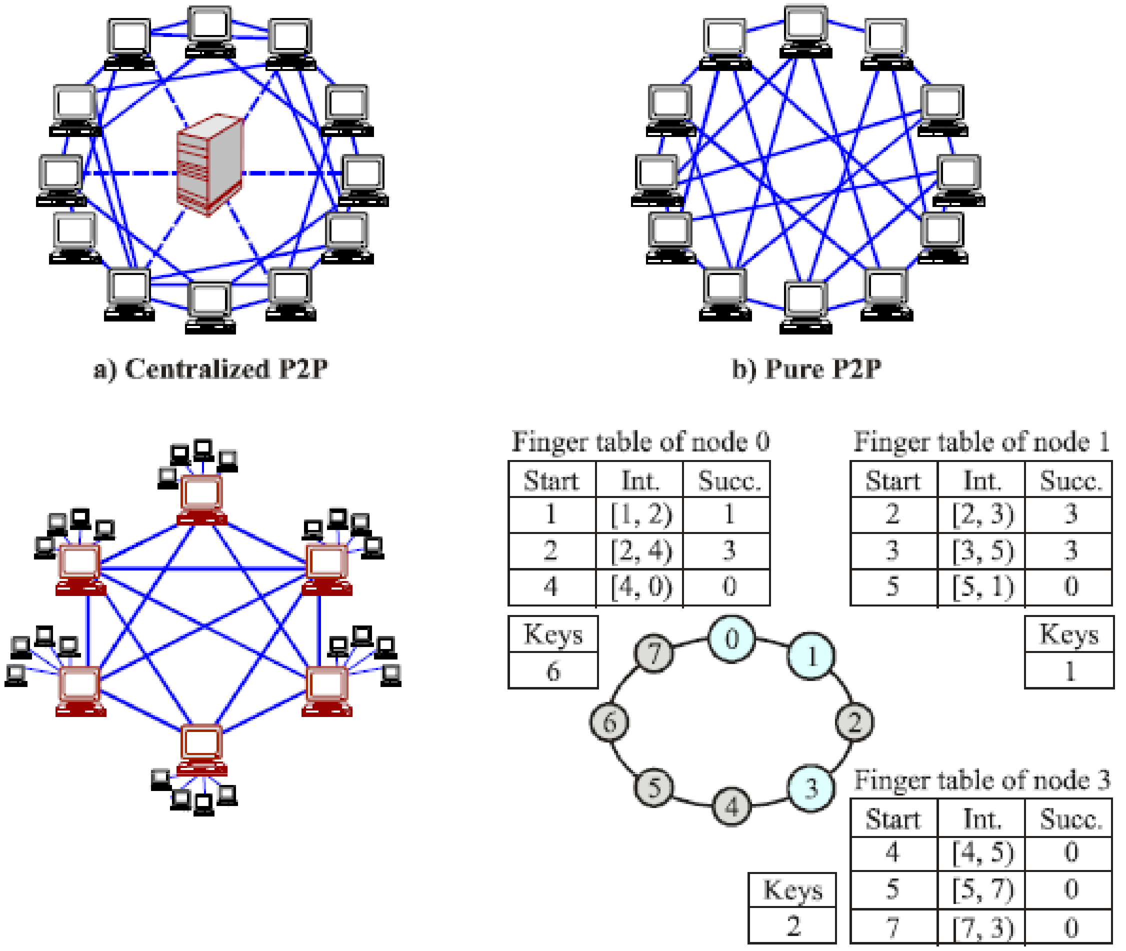
- *X.1111* – Provides framework for home network security
- *X.1143* – Security Architecture for Mobile Messaging Services
- *X.1151* – Guidelines on Secure Password Authentication
- *X.1162* – Security Architecture & Operations for P2P Networks
- *X.1191* – Functional Requirements and Security Architecture for IPTV

……In the following slides we'll give an overview of the reference models for some of these ITU standards. A full analysis of the whole spectrum of ITU cybersecurity standards is beyond the scope of this 2-day workshop

Reference Security Model for Mobile Web Services – X.1143


WSDL, security policy, etc...
Internal domain of an ASP
Application server (non-WS)
Registry server
Discovery service
Mobile terminal (WS or non-WS client)
Internet
ASP's intranet
MWSSG
Application server (WS)
Mobile network
Mobile web services security gateway (MWSSG)
Intranet (wired)
Application server (WS)
Application server (WS)
Core network gateway
Registry server
Policy server
Application server (non-WS)
WSDL, security policy, access control policy...
Internal domain of a mobile network operator
X.1143(07)_FL1

P2P Generic Network Structures – X.1162



a) Centralized P2P

b) Pure P2P

c) Hybrid P2P

d) DHT-based P2P

Finger table of node 0

Start	Int.	Succ.
1	[1, 2)	1
2	[2, 4)	3
4	[4, 0)	0

Keys
6

Finger table of node 1

Start	Int.	Succ.
2	[2, 3)	3
3	[3, 5)	3
5	[5, 1)	0

Keys
1

Finger table of node 3

Start	Int.	Succ.
4	[4, 5)	0
5	[5, 7)	0
7	[7, 3)	0

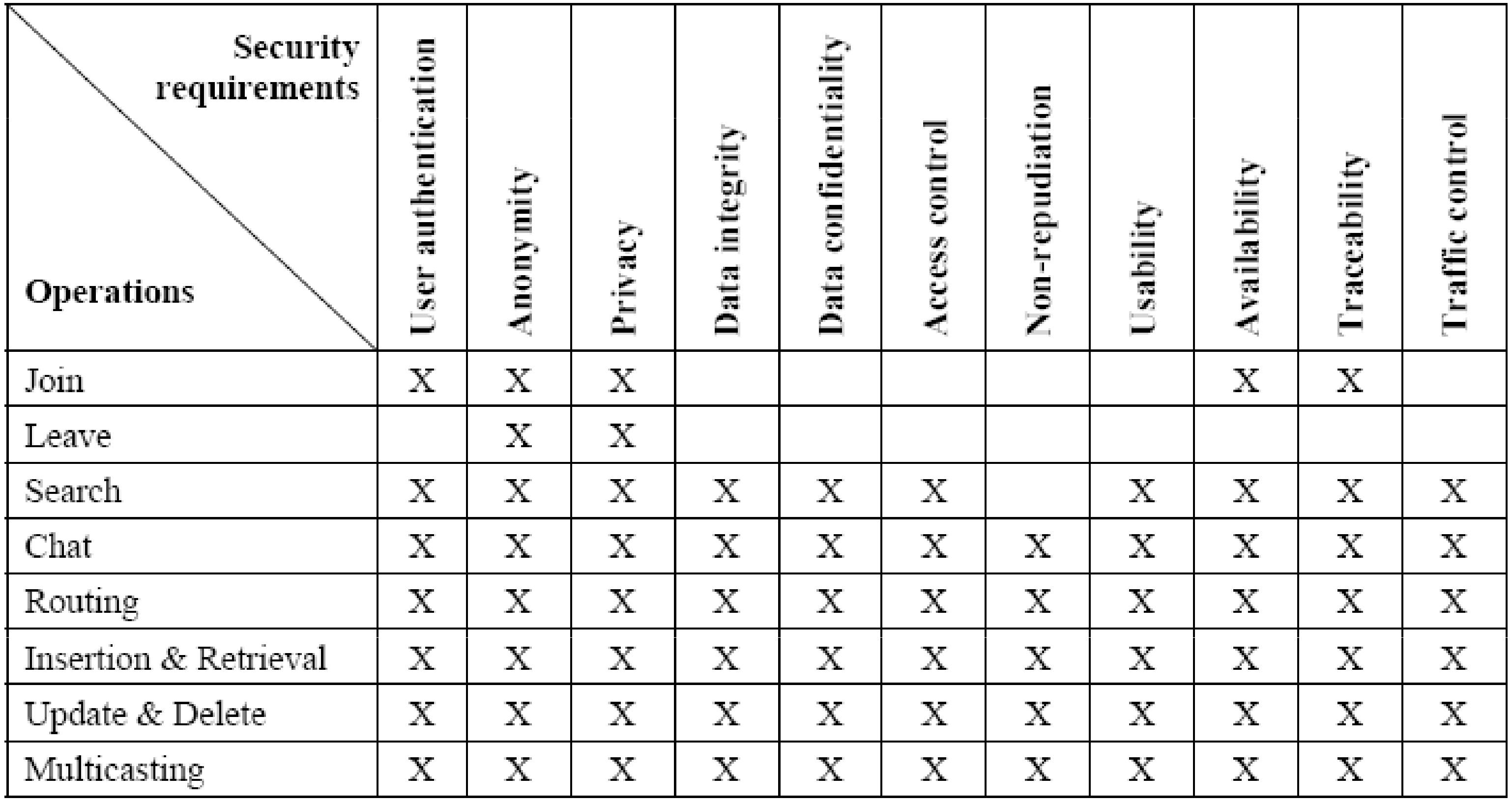
Keys
2

Note: DHT = distributed hash table

X.1162(08)_FA.1

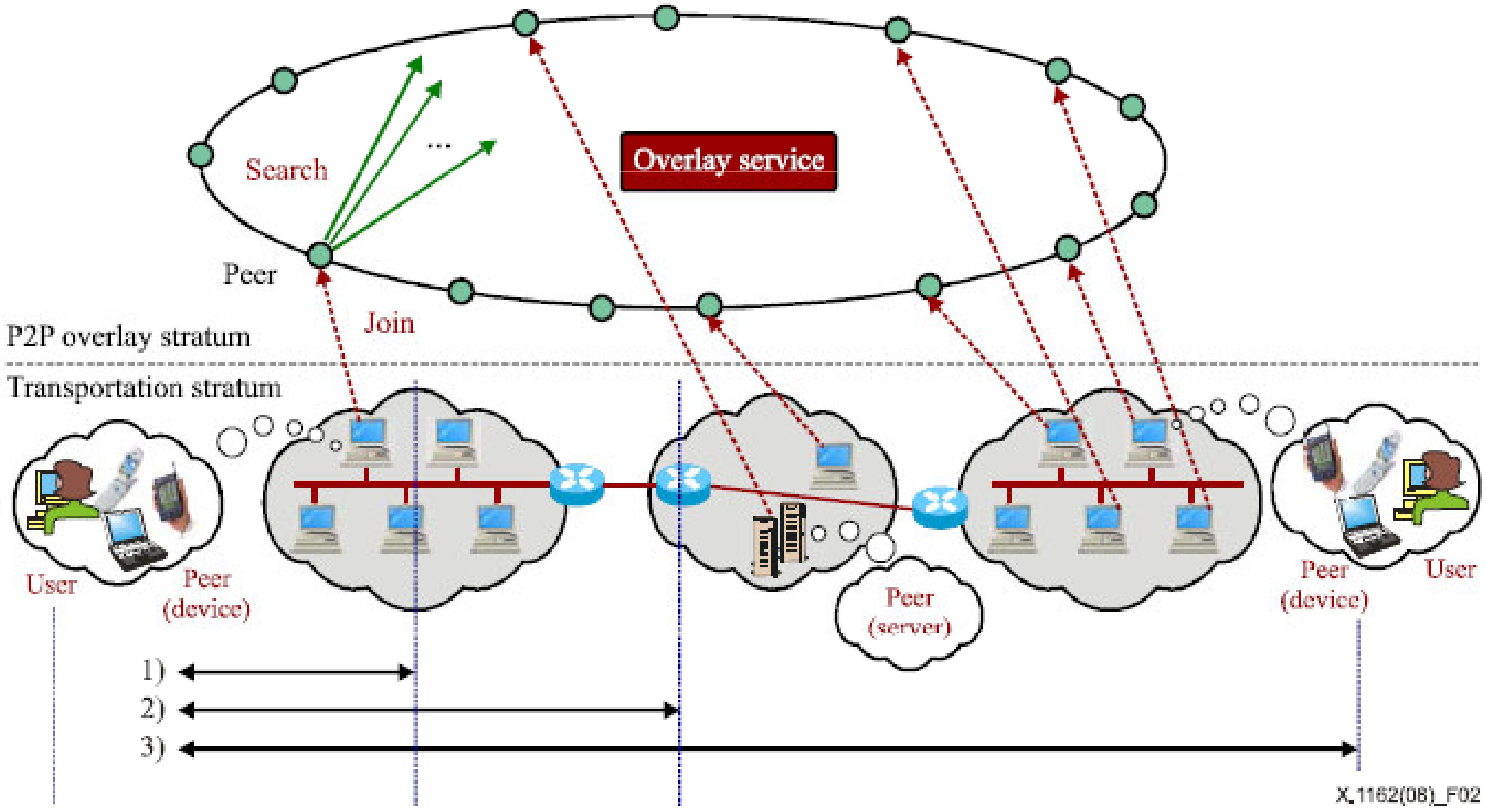
X.1162 - P2P Networks : Security Requirements & Operations

Table 1 – Relationship between security requirements and operations

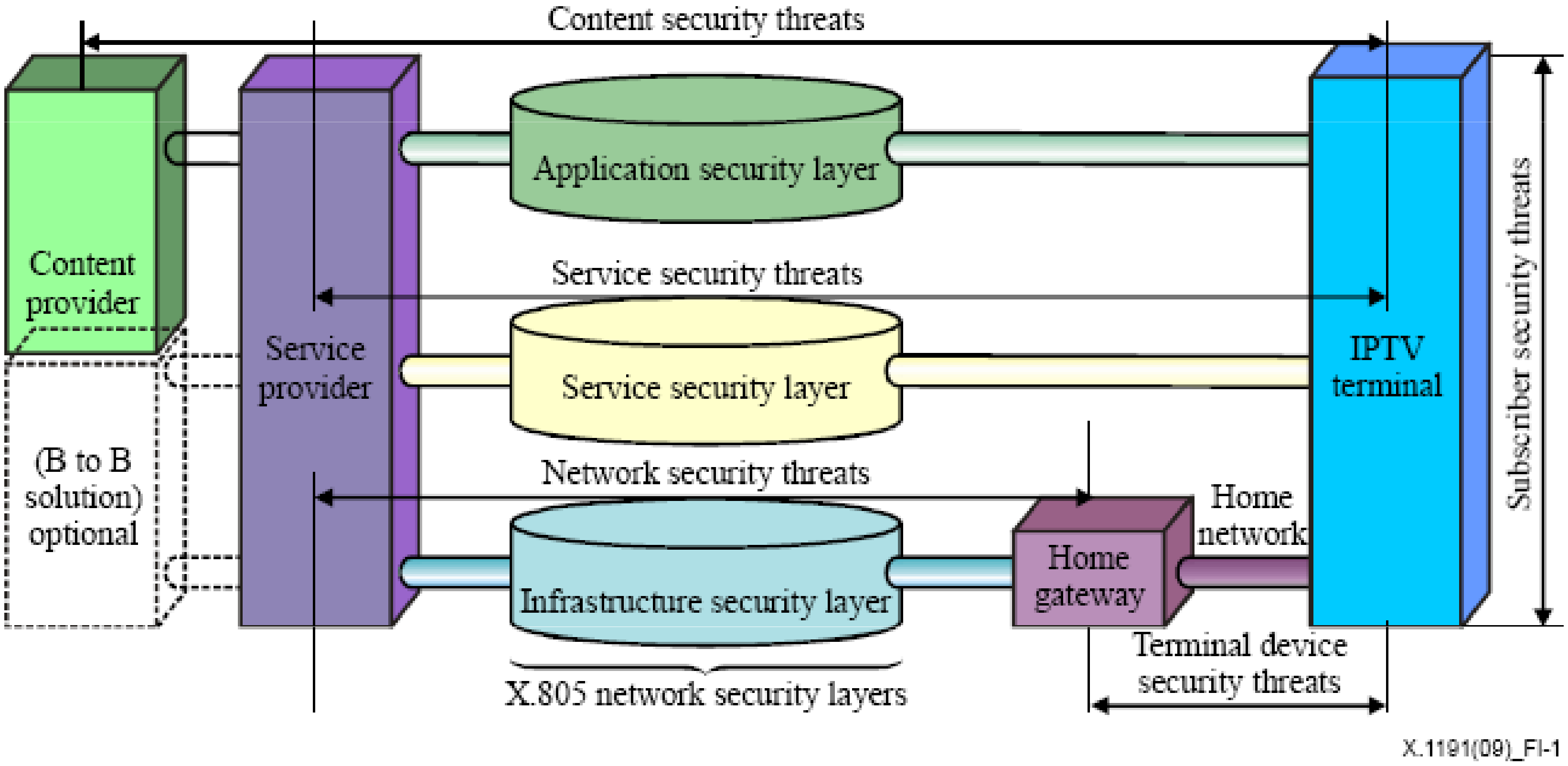


Security requirements / Operations	User authentication	Anonymity	Privacy	Data integrity	Data confidentiality	Access control	Non-repudiation	Usability	Availability	Traceability	Traffic control
Join	X	X	X						X	X	
Leave		X	X								
Search	X	X	X	X	X	X		X	X	X	X
Chat	X	X	X	X	X	X	X	X	X	X	X
Routing	X	X	X	X	X	X	X	X	X	X	X
Insertion & Retrieval	X	X	X	X	X	X	X	X	X	X	X
Update & Delete	X	X	X	X	X	X	X	X	X	X	X
Multicasting	X	X	X	X	X	X	X	X	X	X	X

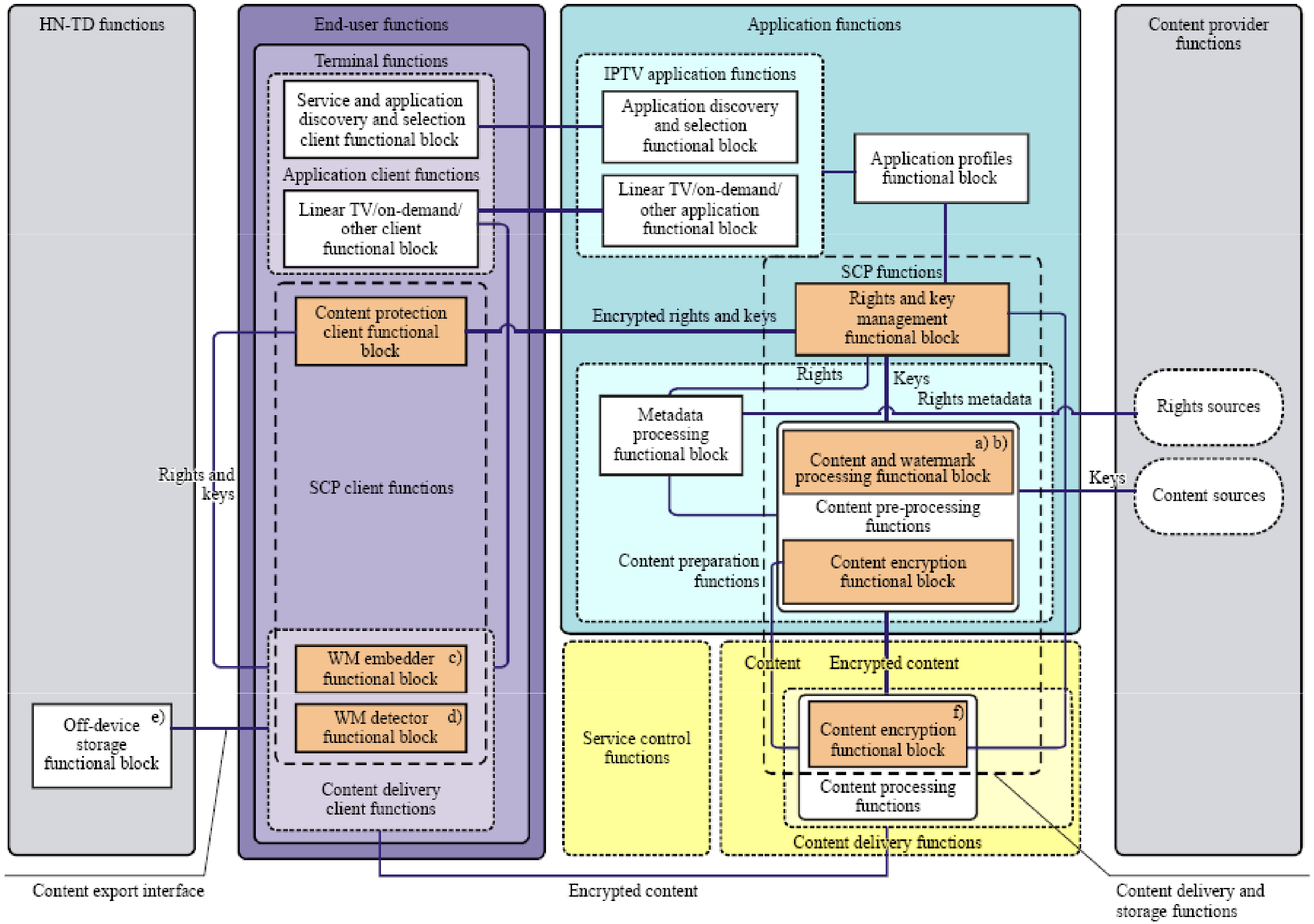
Architectural Model – Peer to Peer Networks



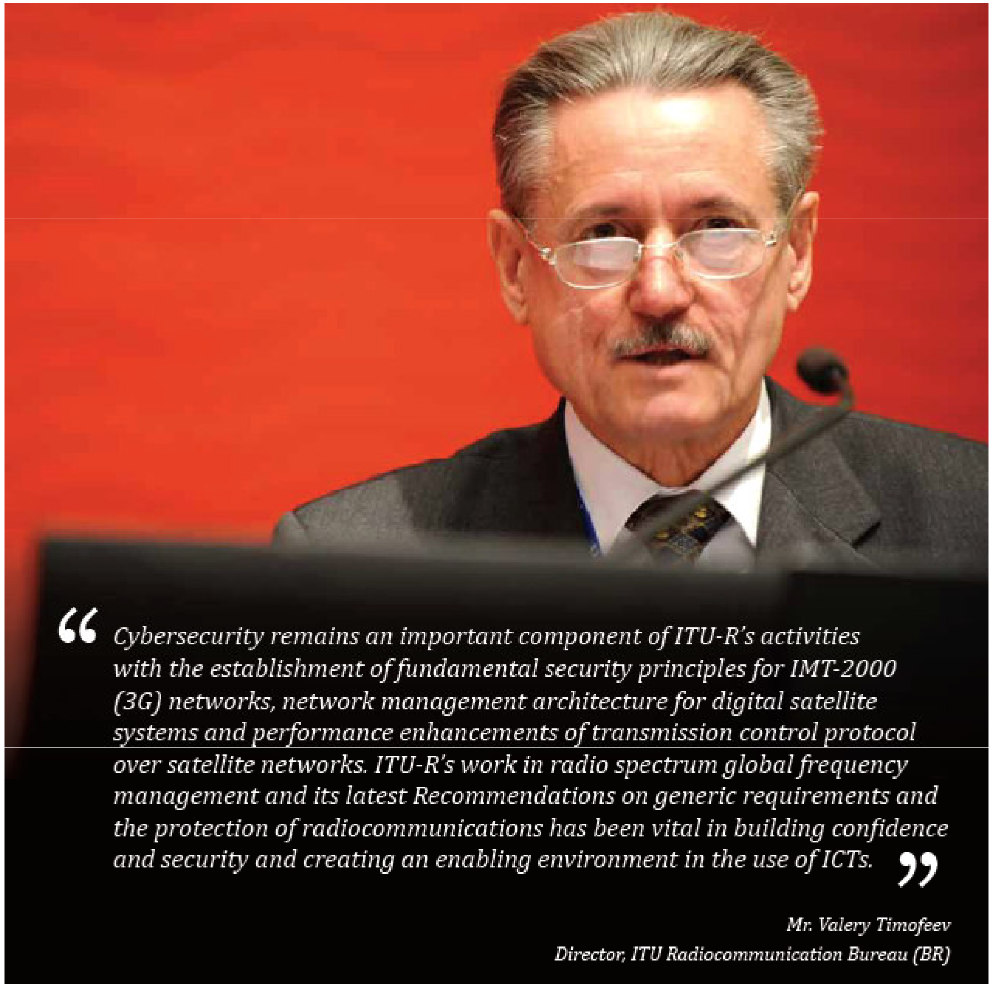
X.1191 - IPTV Security Threats Model



IPTV Protection Architecture – X.1191


HN-TD functions
End-user functions
Terminal functions
Service and application discovery and selection client functional block
Application client functions
Linear TV/on-demand/ other client functional block
Content protection client functional block
SCP client functions
WM embedder functional block c)
WM detector functional block d)
Content delivery client functions
Off-device storage functional block e)
Rights and keys
Application functions
IPTV application functions
Application discovery and selection functional block
Linear TV/on-demand/ other application functional block
Application profiles functional block
SCP functions
Rights and key management functional block
Encrypted rights and keys
Rights
Keys
Rights metadata
Metadata processing functional block
Content and watermark processing functional block a) b)
Content pre-processing functions
Content encryption functional block
Content preparation functions
Service control functions
Content
Encrypted content
Content encryption functional block f)
Content processing functions
Content delivery functions
Content provider functions
Rights sources
Keys
Content sources
Content export interface
Encrypted content
Content delivery and storage functions

Cybersecurity: Director ITU Radiocommunications Bureau (BR)



“Cybersecurity remains an important component of ITU-R’s activities with the establishment of fundamental security principles for IMT-2000 (3G) networks, network management architecture for digital satellite systems and performance enhancements of transmission control protocol over satellite networks. ITU-R’s work in radio spectrum global frequency management and its latest Recommendations on generic requirements and the protection of radiocommunications has been vital in building confidence and security and creating an enabling environment in the use of ICTs.”

Mr. Valery Timofeev
Director, ITU Radiocommunication Bureau (BR)

* Workshop Session 5 *

"Cybersecurity Continuity Planning, Standards and Architectures"

1 – International Standards	2 – ITU Security Standards	3 – ITU: X.805 Architecture
4 – ITU: X1205 CyberSecurity	5 – Others: ISO/IEC & NIST	6 – ISF: Info Security Forum
7 – Practical Implementation	8 – Cyber Continuity: BCP/DR	9 – Next Steps for Jamaica

Other Security Standards: ISO, NIST, ENISA

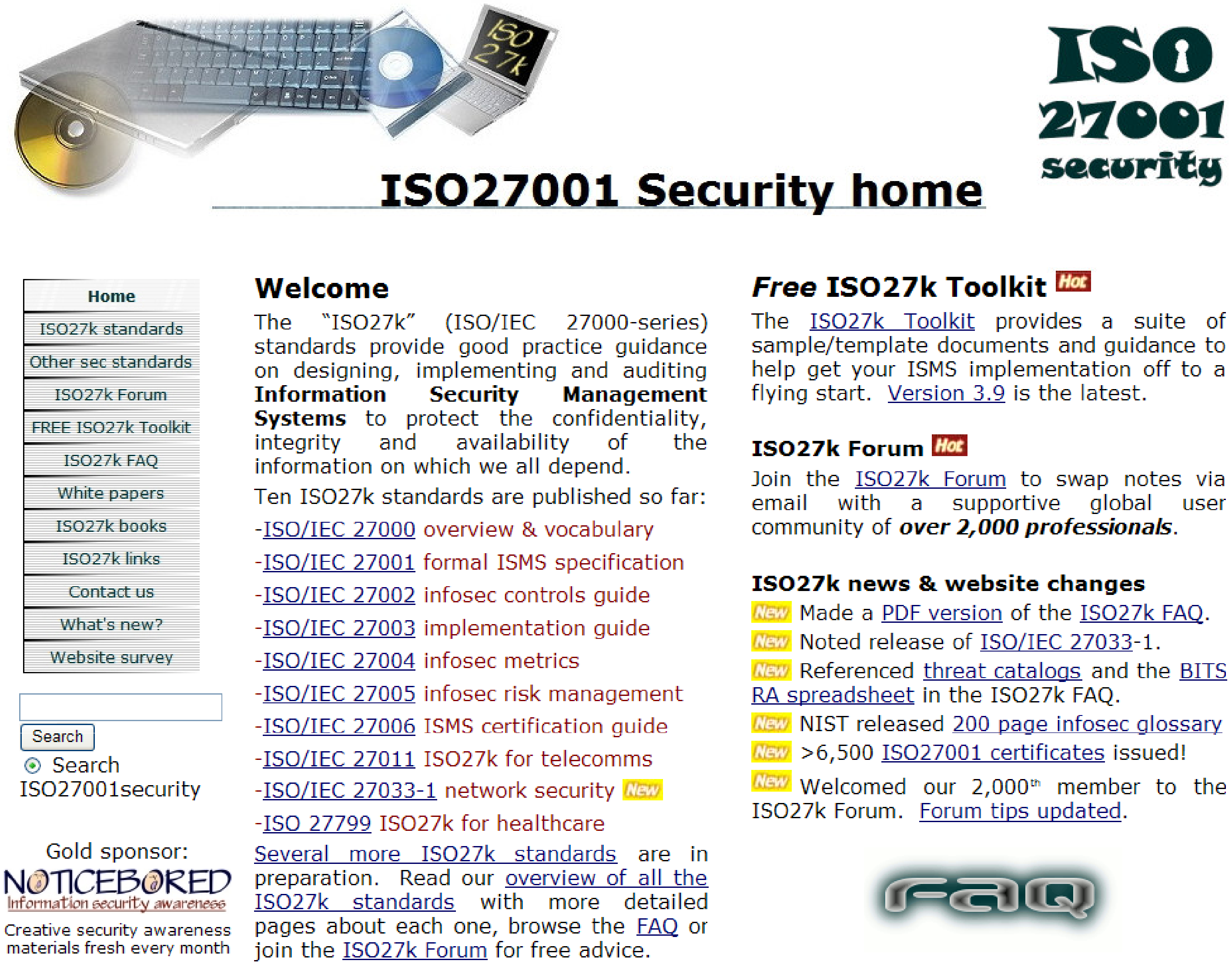
- *ISO/IEC:* These are often adopted as “best practice” for operational aspects of security including the ISO27001 – Information Security Management System, and the ISO27002 – ISMS Code of Practice

- *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

- *IEEE:* An important global player in ICT standards, and a key ITU partner in the development of new standards for open network cybersecurity

ISO27001 Security Standards



ISO27001 Security home

ISO 27001 security

- Home
- ISO27k standards
- Other sec standards
- ISO27k Forum
- FREE ISO27k Toolkit
- ISO27k FAQ
- White papers
- ISO27k books
- ISO27k links
- Contact us
- What's new?
- Website survey

Gold sponsor:
NOTICEBORED Information security awareness
Creative security awareness materials fresh every month

Welcome

The "ISO27k" (ISO/IEC 27000-series) standards provide good practice guidance on designing, implementing and auditing **Information Security Management Systems** to protect the confidentiality, integrity and availability of the information on which we all depend.

Ten ISO27k standards are published so far:

-ISO/IEC 27000 overview & vocabulary

-ISO/IEC 27001 formal ISMS specification

-ISO/IEC 27002 infosec controls guide

-ISO/IEC 27003 implementation guide

-ISO/IEC 27004 infosec metrics

-ISO/IEC 27005 infosec risk management

-ISO/IEC 27006 ISMS certification guide

-ISO/IEC 27011 ISO27k for telecomms

-ISO/IEC 27033-1 network security New

-ISO 27799 ISO27k for healthcare

Several more ISO27k standards are in preparation. Read our overview of all the ISO27k standards with more detailed pages about each one, browse the FAQ or join the ISO27k Forum for free advice.

Free ISO27k Toolkit Hot

The ISO27k Toolkit provides a suite of sample/template documents and guidance to help get your ISMS implementation off to a flying start. Version 3.9 is the latest.

ISO27k Forum Hot

Join the ISO27k Forum to swap notes via email with a supportive global user community of ***over 2,000 professionals***.

ISO27k news & website changes

New Made a PDF version of the ISO27k FAQ.

New Noted release of ISO/IEC 27033-1.

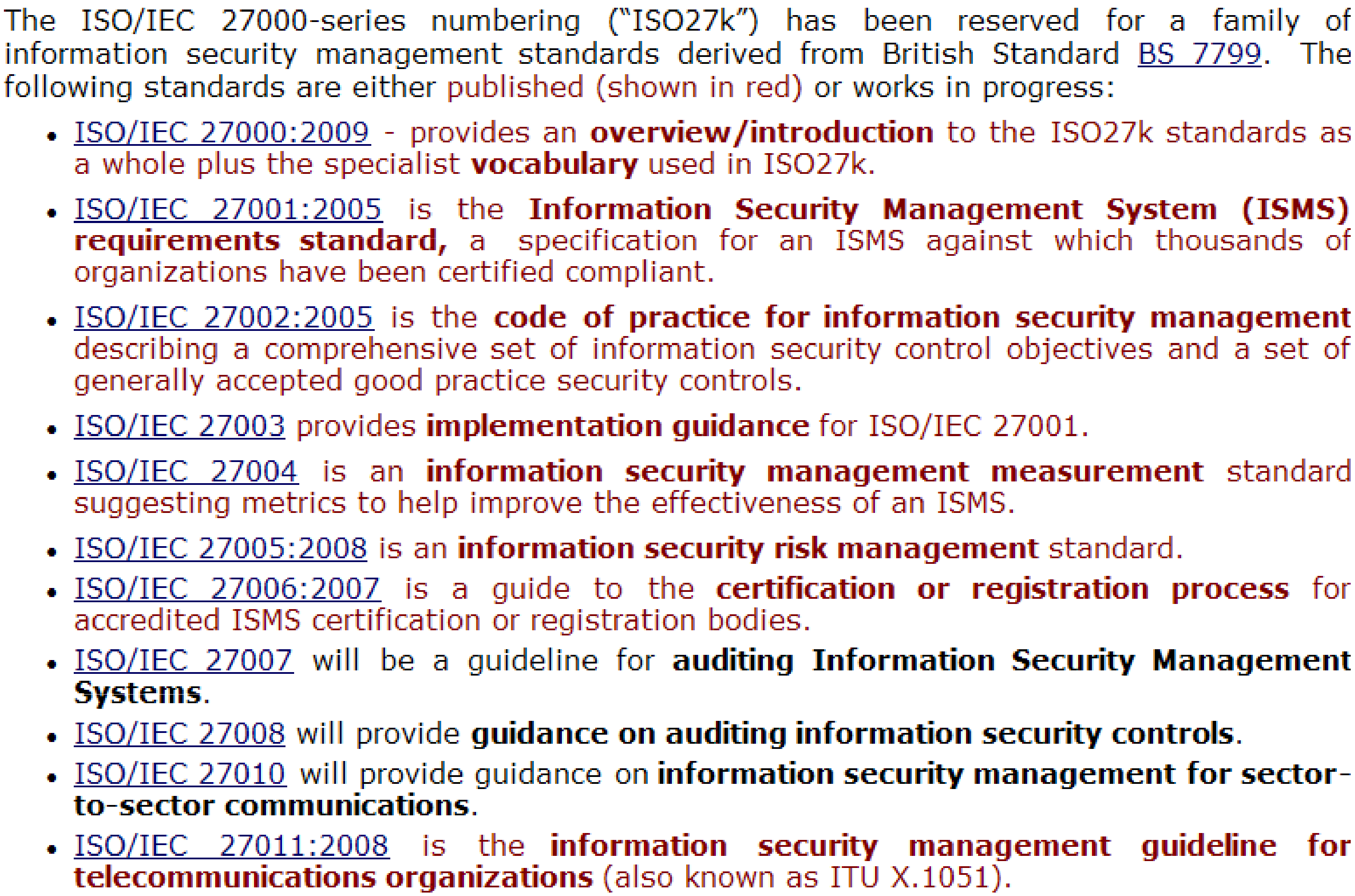
New Referenced threat catalogs and the BITS RA spreadsheet in the ISO27k FAQ.

New NIST released 200 page infosec glossary

New >6,500 ISO27001 certificates issued!

New Welcomed our 2,000th member to the ISO27k Forum. Forum tips updated.

ISO/IEC 27000-Series



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 (ISMS – ISO 27001)

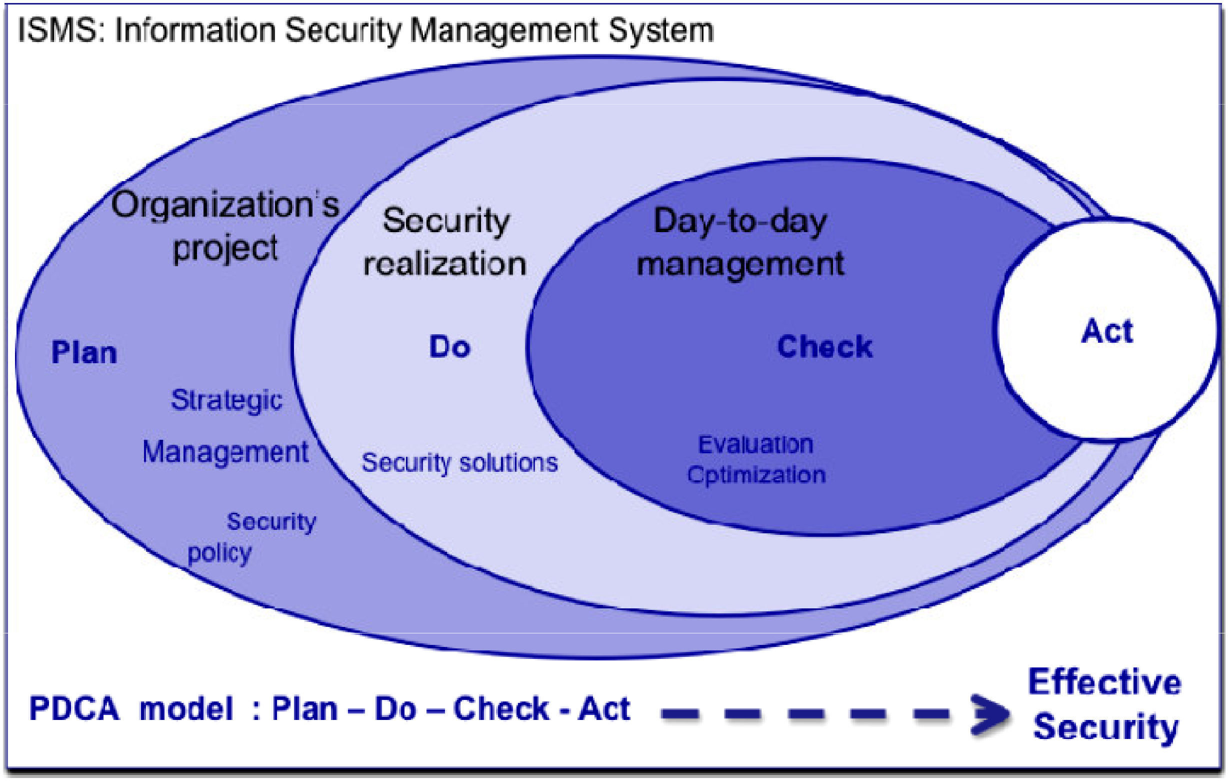
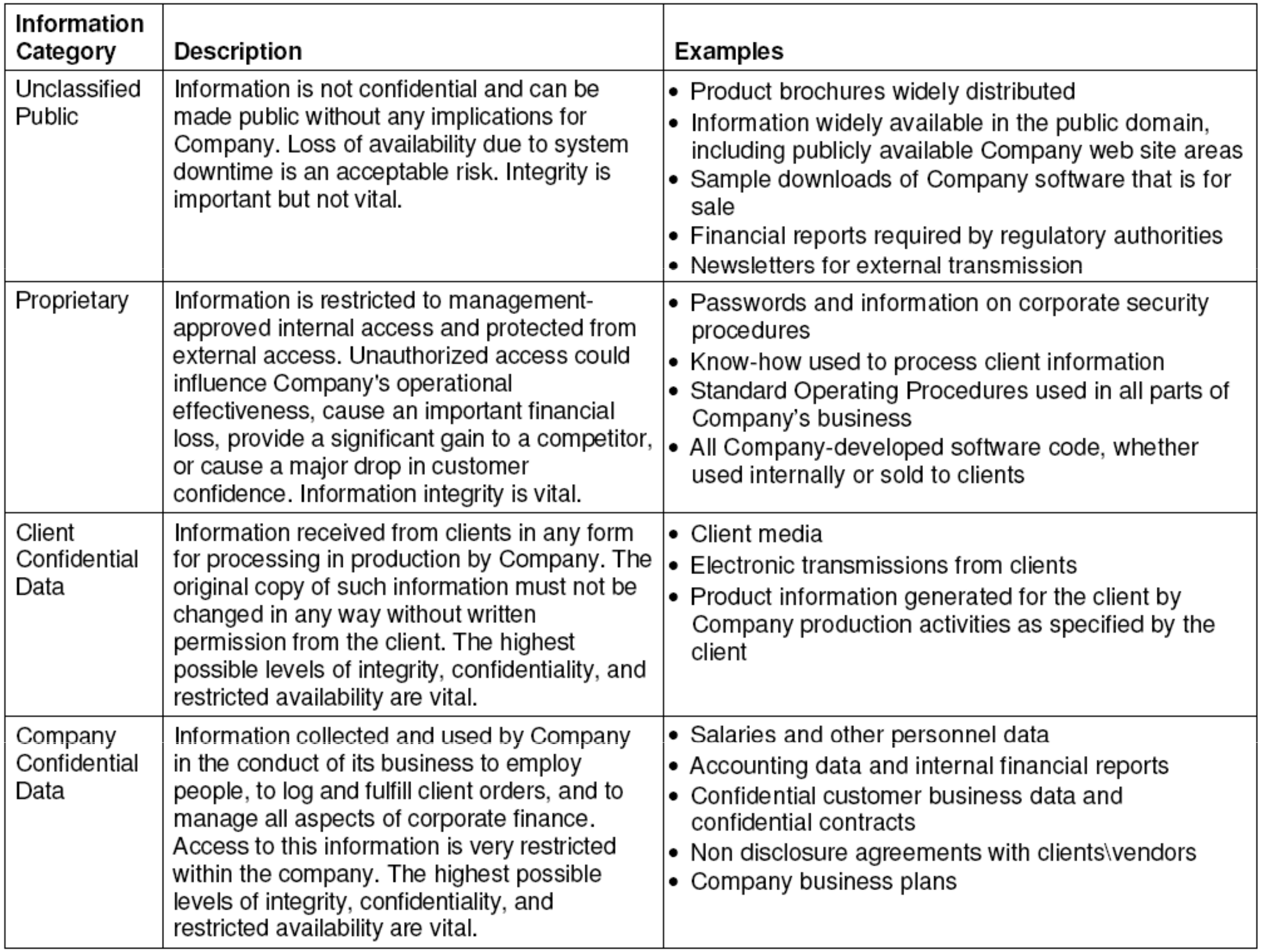


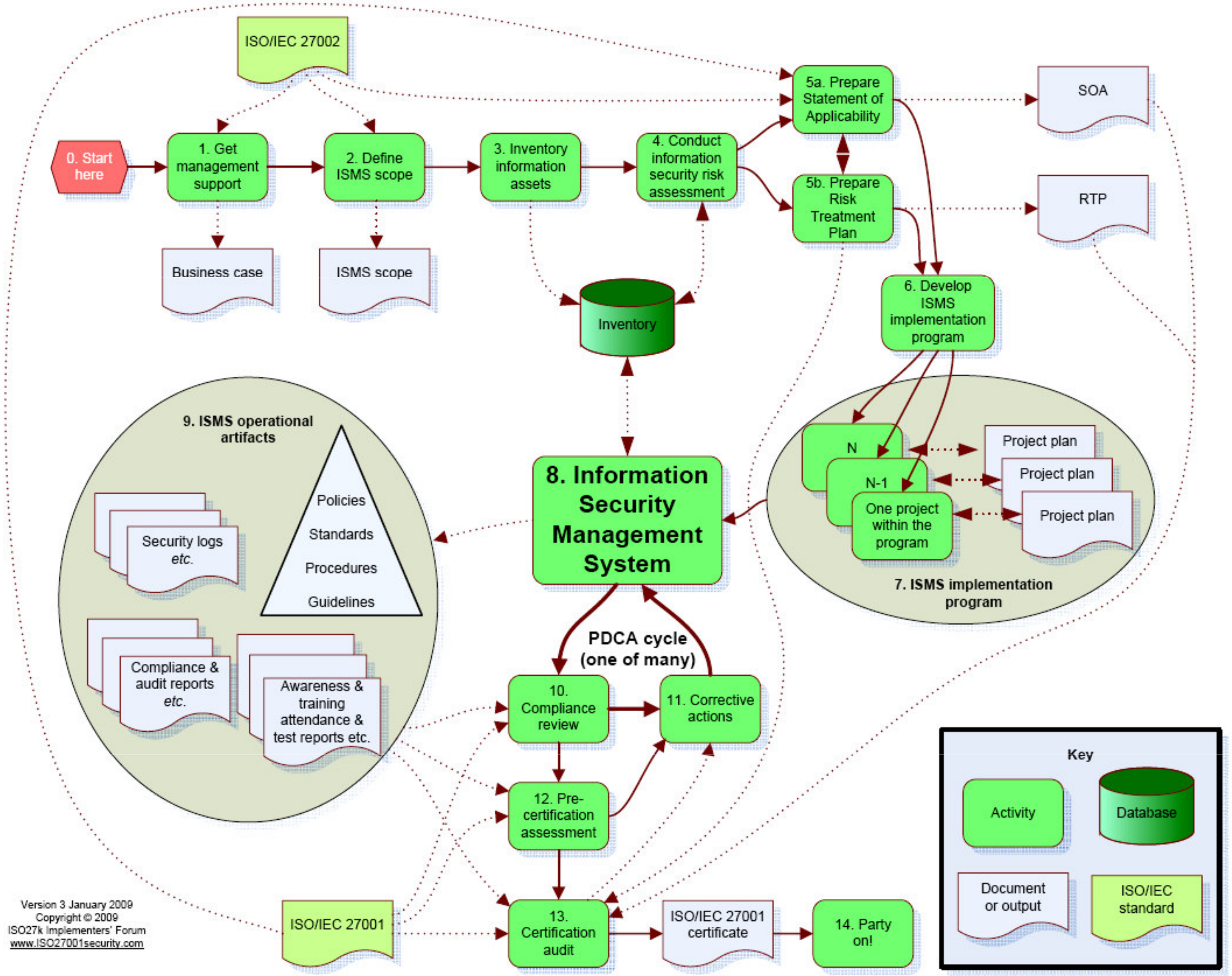
Figure V.10: Information Security Management System

Example: ISMS Information Classification Policy



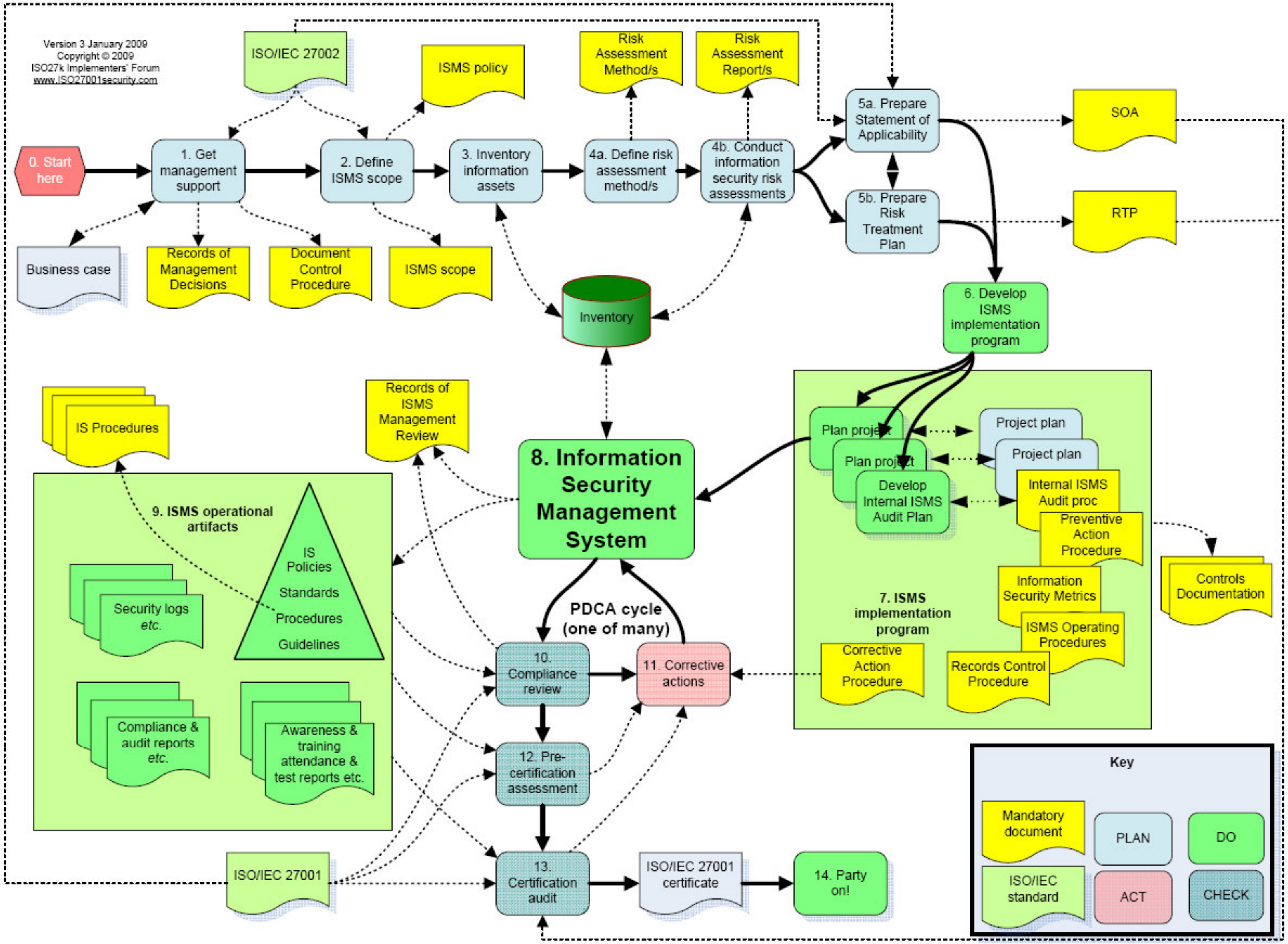
Information Category	Description	Examples
Unclassified Public	Information is not confidential and can be made public without any implications for Company. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital.	• Product brochures widely distributed • Information widely available in the public domain, including publicly available Company web site areas • Sample downloads of Company software that is for sale • Financial reports required by regulatory authorities • Newsletters for external transmission
Proprietary	Information is restricted to management-approved internal access and protected from external access. Unauthorized access could influence Company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	• Passwords and information on corporate security procedures • Know-how used to process client information • Standard Operating Procedures used in all parts of Company's business • All Company-developed software code, whether used internally or sold to clients
Client Confidential Data	Information received from clients in any form for processing in production by Company. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Client media • Electronic transmissions from clients • Product information generated for the client by Company production activities as specified by the client
Company Confidential Data	Information collected and used by Company in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Salaries and other personnel data • Accounting data and internal financial reports • Confidential customer business data and confidential contracts • Non disclosure agreements with clients\vendors • Company business plans

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 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

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

5a. Prepare Statement of Applicability

5b. Prepare Risk Treatment Plan

SOA

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

9. ISMS operational artifacts

IS Policies

Standards

Procedures

Guidelines

Security logs *etc.*

Compliance & audit reports *etc.*

Awareness & training attendance & test reports etc.

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!

Plan project

Plan project

Develop Internal ISMS Audit Plan

Project plan

Project plan

Internal ISMS Audit proc

Preventive Action Procedure

Information Security Metrics

ISMS Operating Procedures

7. ISMS implementation program

Corrective Action Procedure

Records Control Procedure

Controls Documentation

Key

Mandatory document

PLAN

DO

ISO/IEC standard

ACT

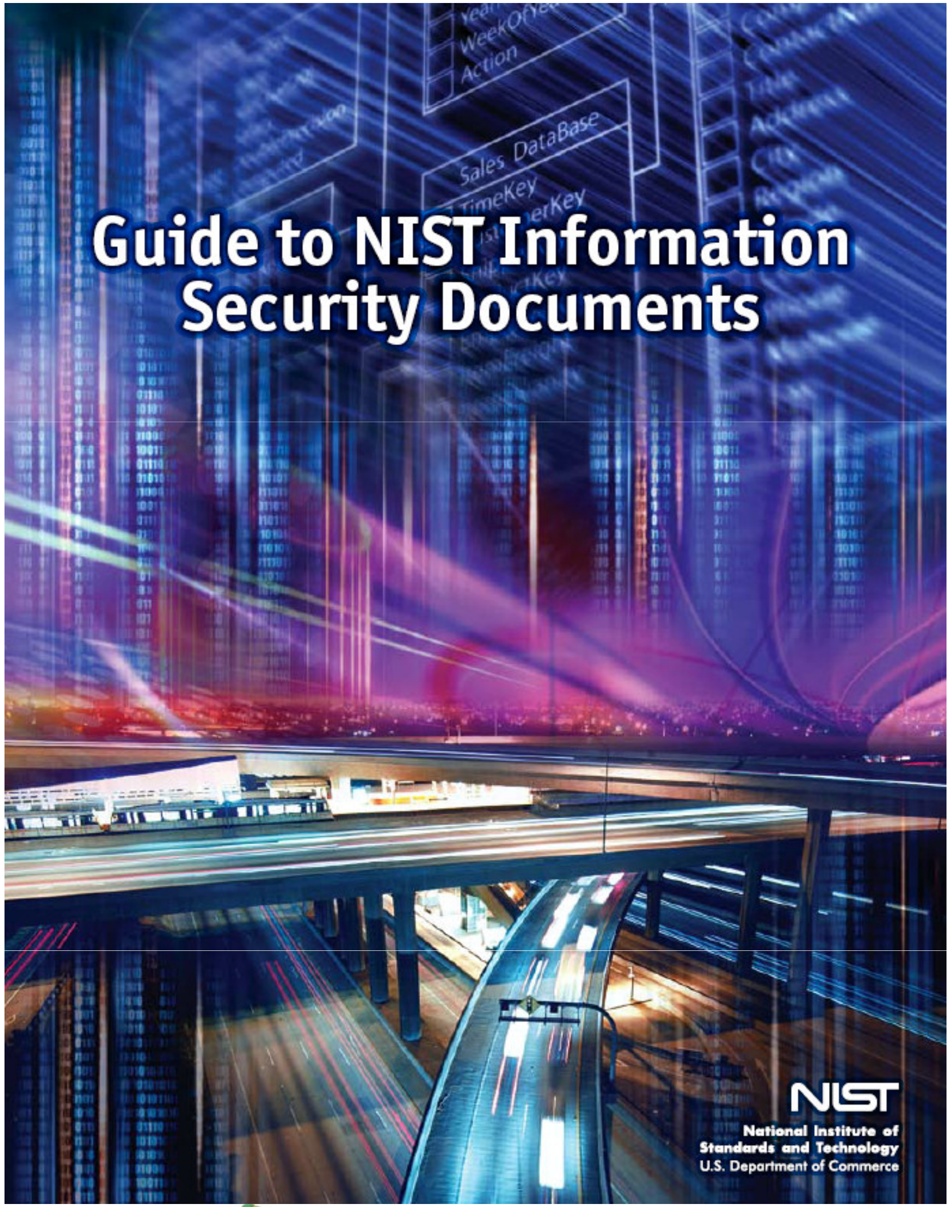
CHECK

University of Technology, Jamaica

ITU Centres of Excellence Network for the Caribbean Region
Cybersecurity Technologies, Standards & Operations
16-17 September, Kingston, Jamaica

International Telecommunication Union
Committed to connecting the world

NIST Security Publications: “800 Series”



Guide to NIST Information Security Documents

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

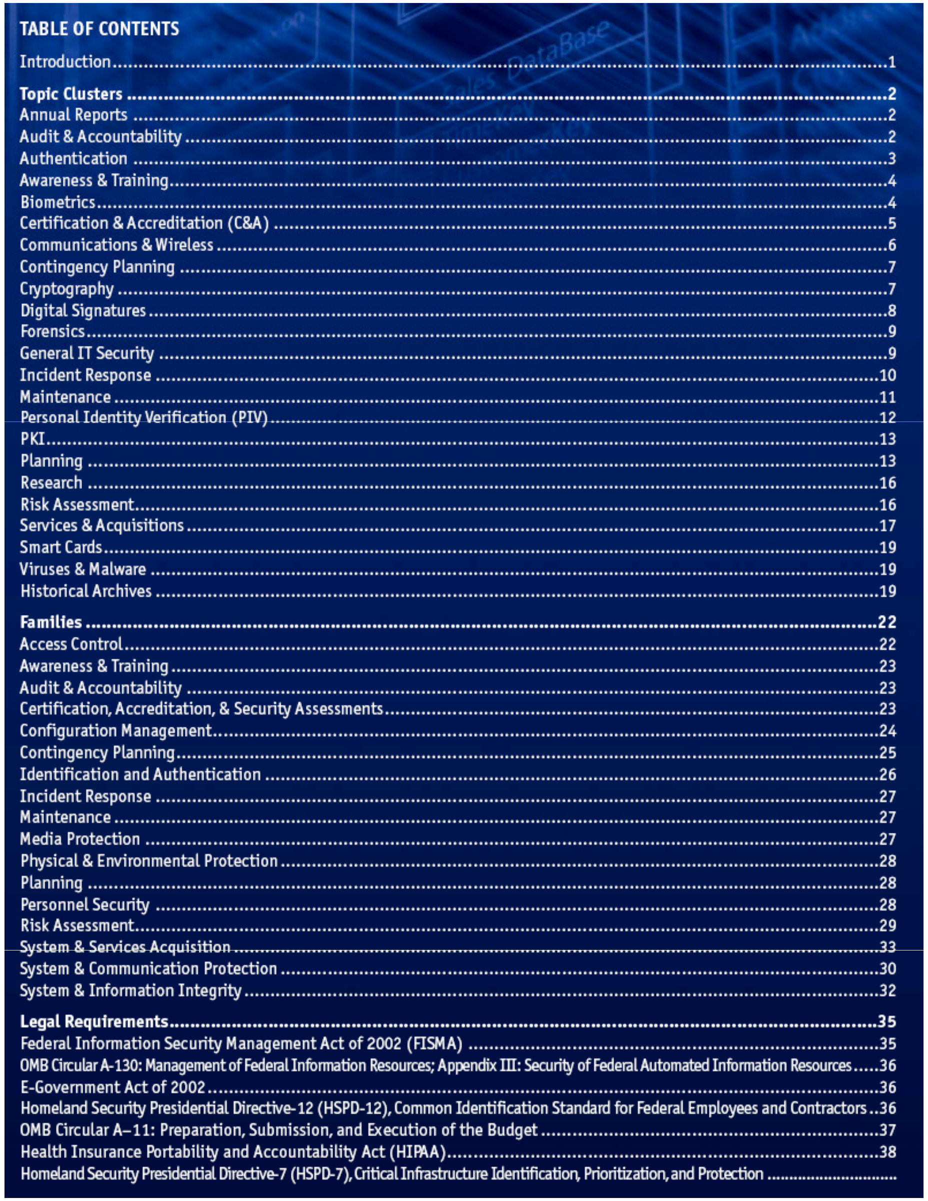


TABLE OF CONTENTS

Introduction 1

Topic Clusters 2
Annual Reports 2
Audit & Accountability 2
Authentication 3
Awareness & Training 4
Biometrics 4
Certification & Accreditation (C&A) 5
Communications & Wireless 6
Contingency Planning 7
Cryptography 7
Digital Signatures 8
Forensics 9
General IT Security 9
Incident Response 10
Maintenance 11
Personal Identity Verification (PIV) 12
PKI 13
Planning 13
Research 16
Risk Assessment 16
Services & Acquisitions 17
Smart Cards 19
Viruses & Malware 19
Historical Archives 19

Families 22
Access Control 22
Awareness & Training 23
Audit & Accountability 23
Certification, Accreditation, & Security Assessments 23
Configuration Management 24
Contingency Planning 25
Identification and Authentication 26
Incident Response 27
Maintenance 27
Media Protection 27
Physical & Environmental Protection 28
Planning 28
Personnel Security 28
Risk Assessment 29
System & Services Acquisition 33
System & Communication Protection 30
System & Information Integrity 32

Legal Requirements 35
Federal Information Security Management Act of 2002 (FISMA) 35
OMB Circular A-130: Management of Federal Information Resources; Appendix III: Security of Federal Automated Information Resources 36
E-Government Act of 2002 36
Homeland Security Presidential Directive-12 (HSPD-12), Common Identification Standard for Federal Employees and Contractors ..36
OMB Circular A–11: Preparation, Submission, and Execution of the Budget 37
Health Insurance Portability and Accountability Act (HIPAA) 38
Homeland Security Presidential Directive-7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection ....

NIST Publications: Security Topics

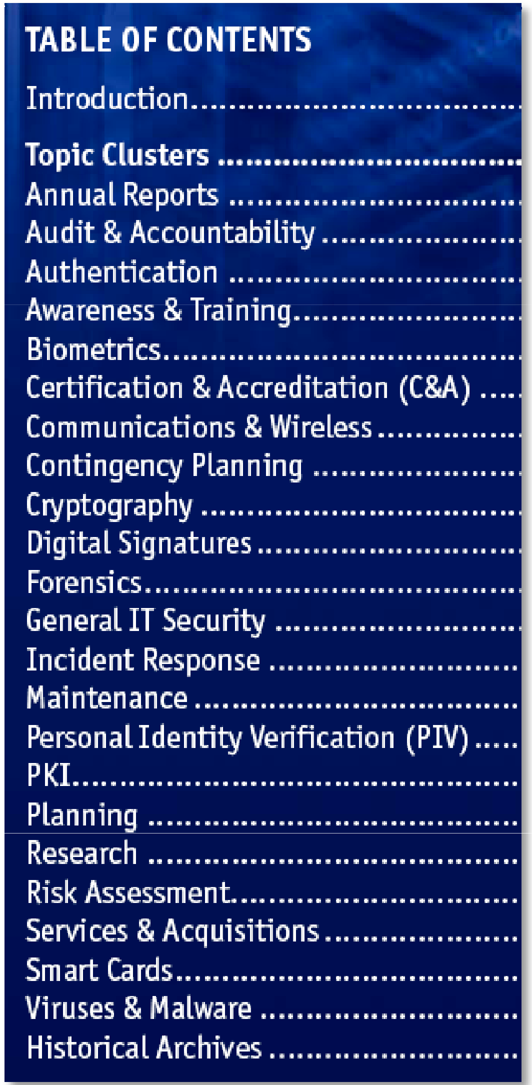
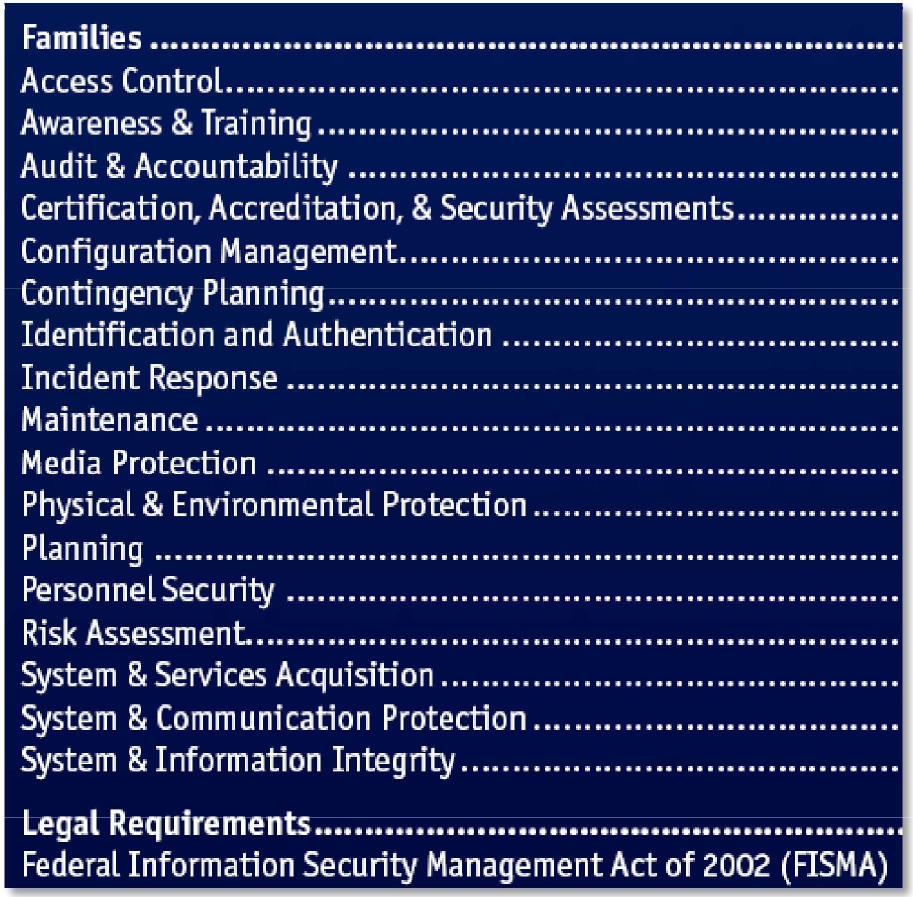


TABLE OF CONTENTS

Introduction

Topic Clusters

- Annual Reports
- Audit & Accountability
- Authentication
- Awareness & Training
- Biometrics
- Certification & Accreditation (C&A)
- Communications & Wireless
- Contingency Planning
- Cryptography
- Digital Signatures
- Forensics
- General IT Security
- Incident Response
- Maintenance
- Personal Identity Verification (PIV)
- PKI
- Planning
- Research
- Risk Assessment
- Services & Acquisitions
- Smart Cards
- Viruses & Malware
- Historical Archives



Families

- Access Control
- Awareness & Training
- Audit & Accountability
- Certification, Accreditation, & Security Assessments
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical & Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System & Services Acquisition
- System & Communication Protection
- System & Information Integrity

Legal Requirements

- Federal Information Security Management Act of 2002 (FISMA)

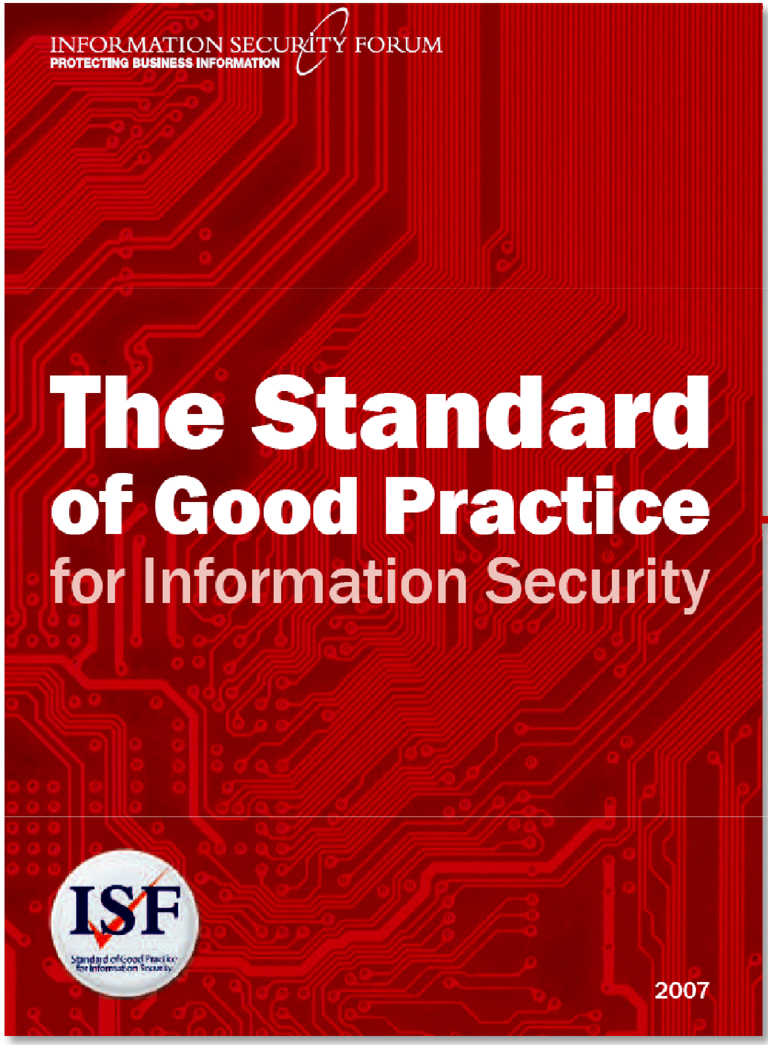
NIST Computer Security Division: csrc.nist.gov

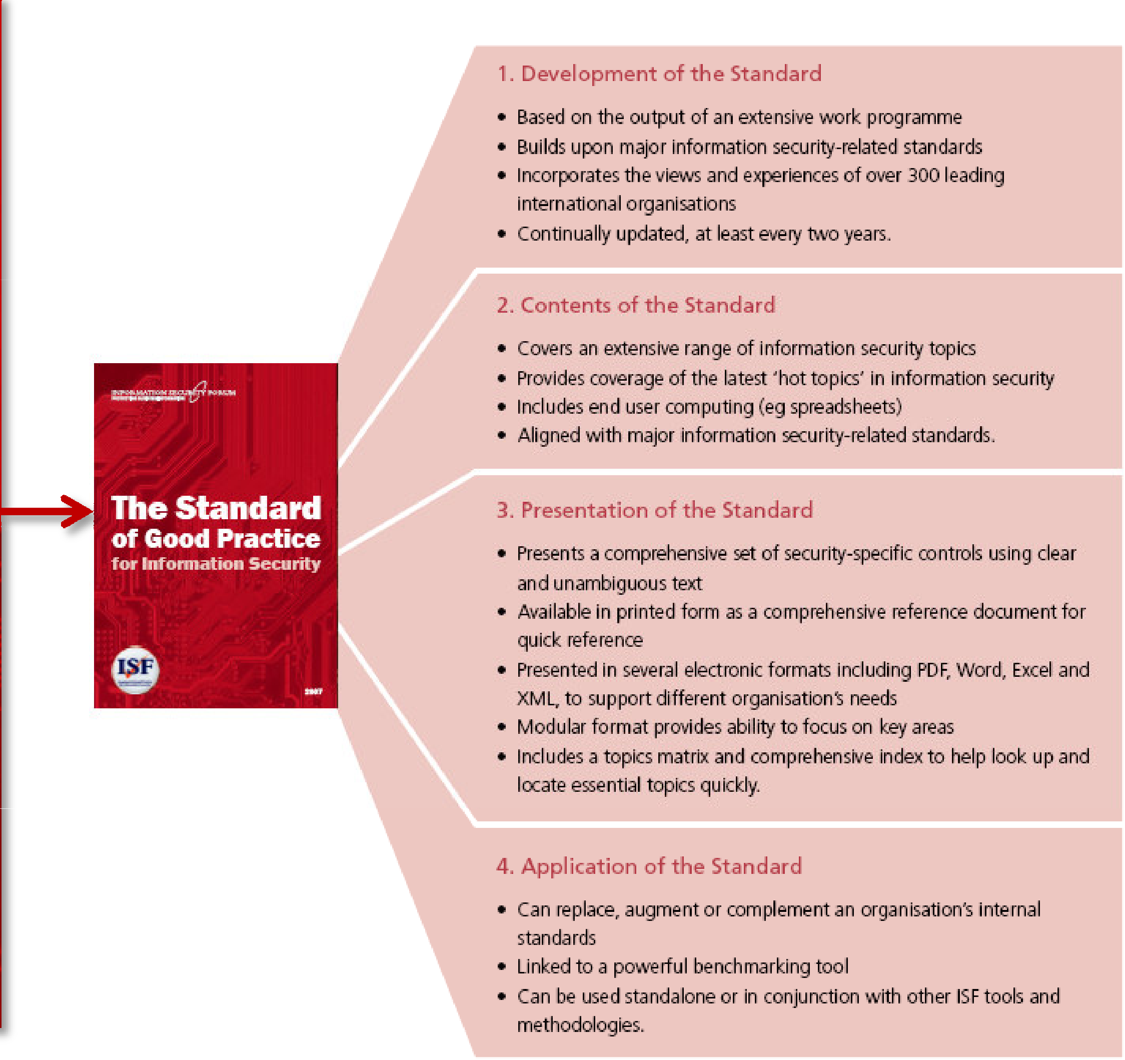
* Workshop Session 5 *

"Cybersecurity Continuity Planning, Standards and Architectures"

1 – International Standards	2 – ITU Security Standards	3 – ITU: X.805 Architecture
4 – ITU: X1205 CyberSecurity	5 – Others: ISO/IEC & NIST	6 – ISF: Info Security Forum
7 – Practical Implementation	8 – Cyber Continuity: BCP/DR	9 – Next Steps for Jamaica

ISF: Information Security Forum


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


INFORMATION SECURITY FORUM
The Standard of Good Practice for Information Security
ISF
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.

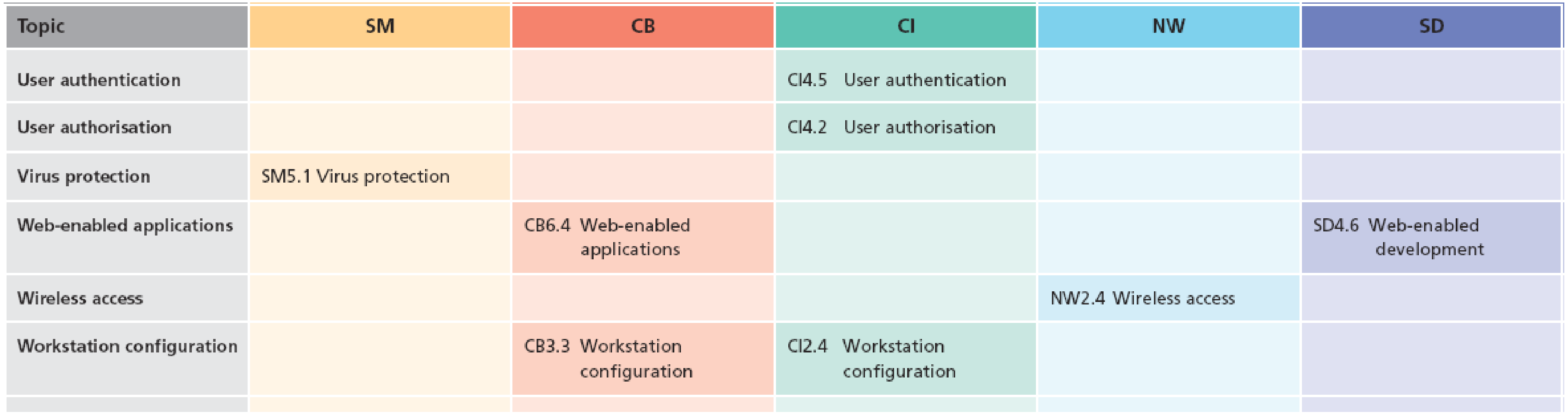
3. Presentation of the Standard

- 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.

Info Security Forum Matrix – (1)



Topic	SM	CB	CI	NW	SD
User authentication			CI4.5 User authentication		
User authorisation			CI4.2 User authorisation		
Virus protection	SM5.1 Virus protection				
Web-enabled applications		CB6.4 Web-enabled applications			SD4.6 Web-enabled development
Wireless access				NW2.4 Wireless access	
Workstation configuration		CB3.3 Workstation configuration	CI2.4 Workstation configuration		

SM = Security Management
CB = Critical Business Applications
CI = Computer Installations
NW = Networks
SD = Systems Development

University of Technology, Jamaica

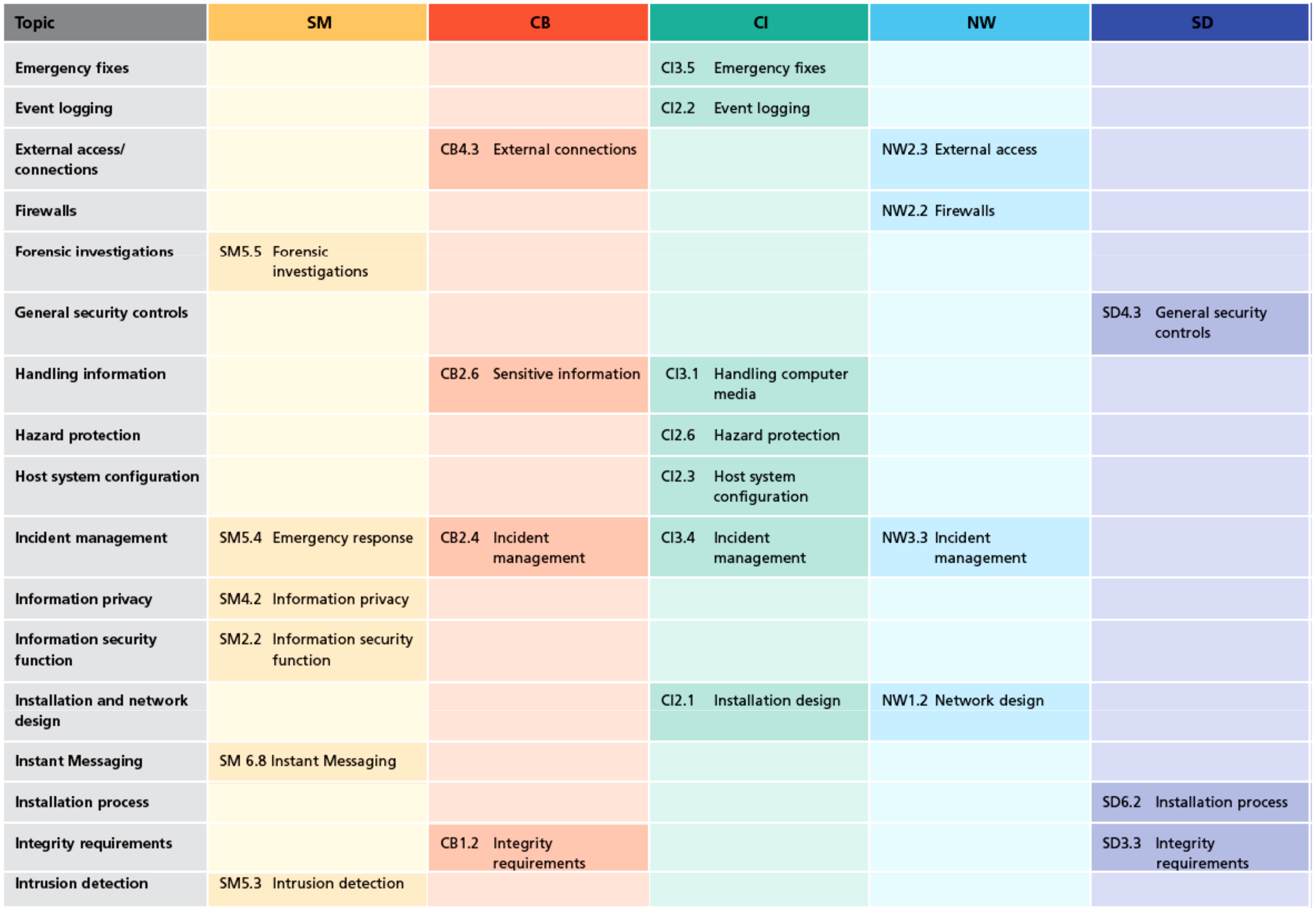
International Telecommunication Union

Committed to connecting the world

Info Security Forum Matrix – (2)

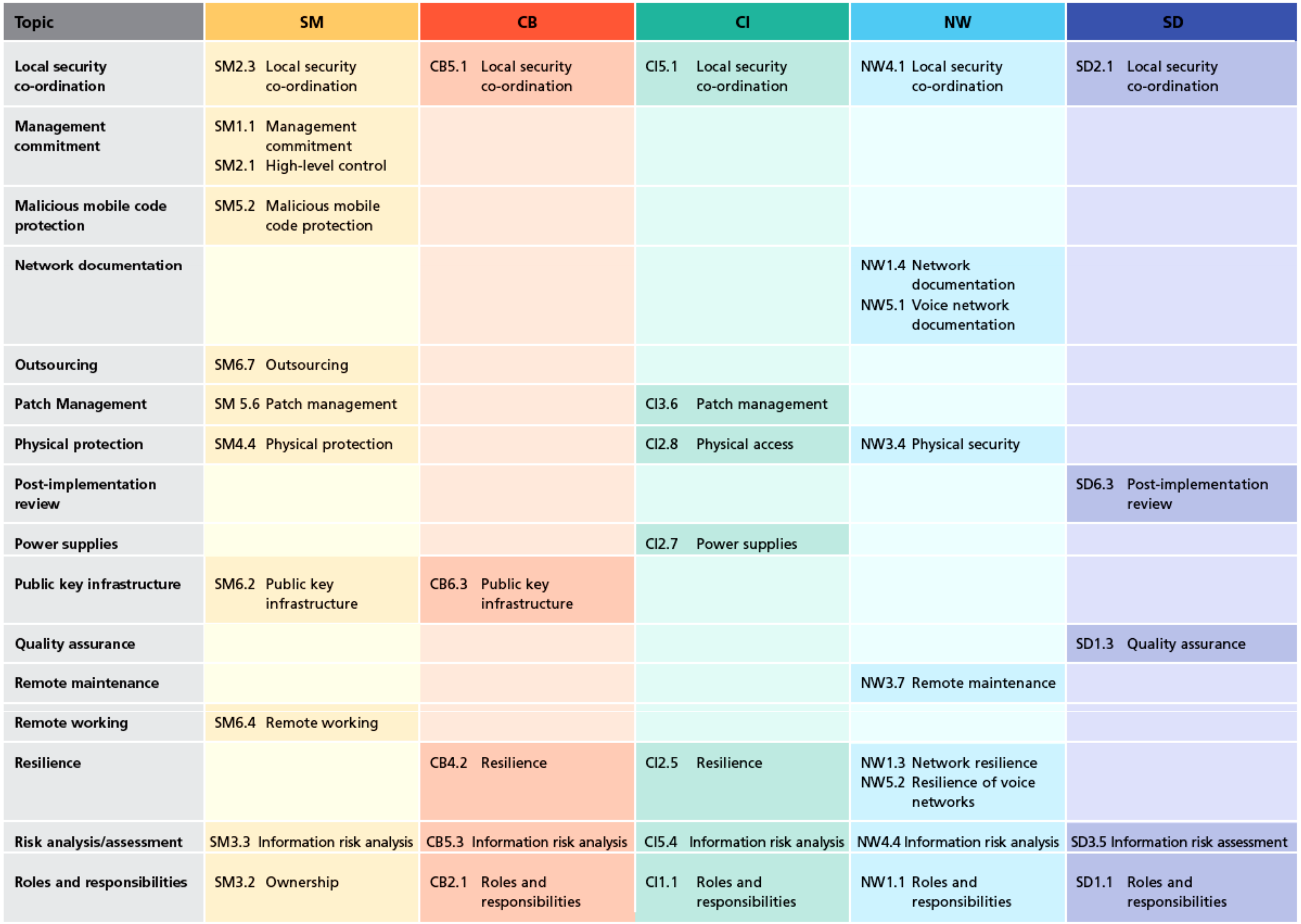
Topic	SM	CB	CI	NW	SD
Access control		CB3.1 Access control	CI4.1 Access control arrangements CI4.3 Access privileges		
Acquisition					SD4.4 Acquisition
Application controls		CB2.2 Application controls			SD4.2 Application controls
Asset management	SM4.3 Asset management		CI1.3 Asset management		
Availability requirements		CB1.3 Availability requirements			SD3.4 Availability requirements
Back-up		CB4.4 Back-up	CI3.2 Back-up	NW3.5 Back-up	
Business continuity	SM4.5 Business continuity	CB2.5 Business continuity	CI6.1 Contingency plan CI6.2 Contingency arrangements CI6.3 Validation and maintenance	NW3.6 Service continuity	
Change management		CB2.3 Change management	CI3.3 Change management	NW3.2 Change management	
Confidentiality requirements		CB1.1 Confidentiality requirements			SD3.2 Confidentiality requirements
Configuring network devices				NW2.1 Configuring network devices	
Cryptography	SM6.1 Use of cryptography	CB6.2 Cryptographic key management			
Development methodologies and environment					SD1.2 Development methodology SD1.4 Development environments
E-mail	SM6.3 E-mail				
Electronic commerce	SM6.6 Electronic commerce				

Info Security Forum Matrix – (3)



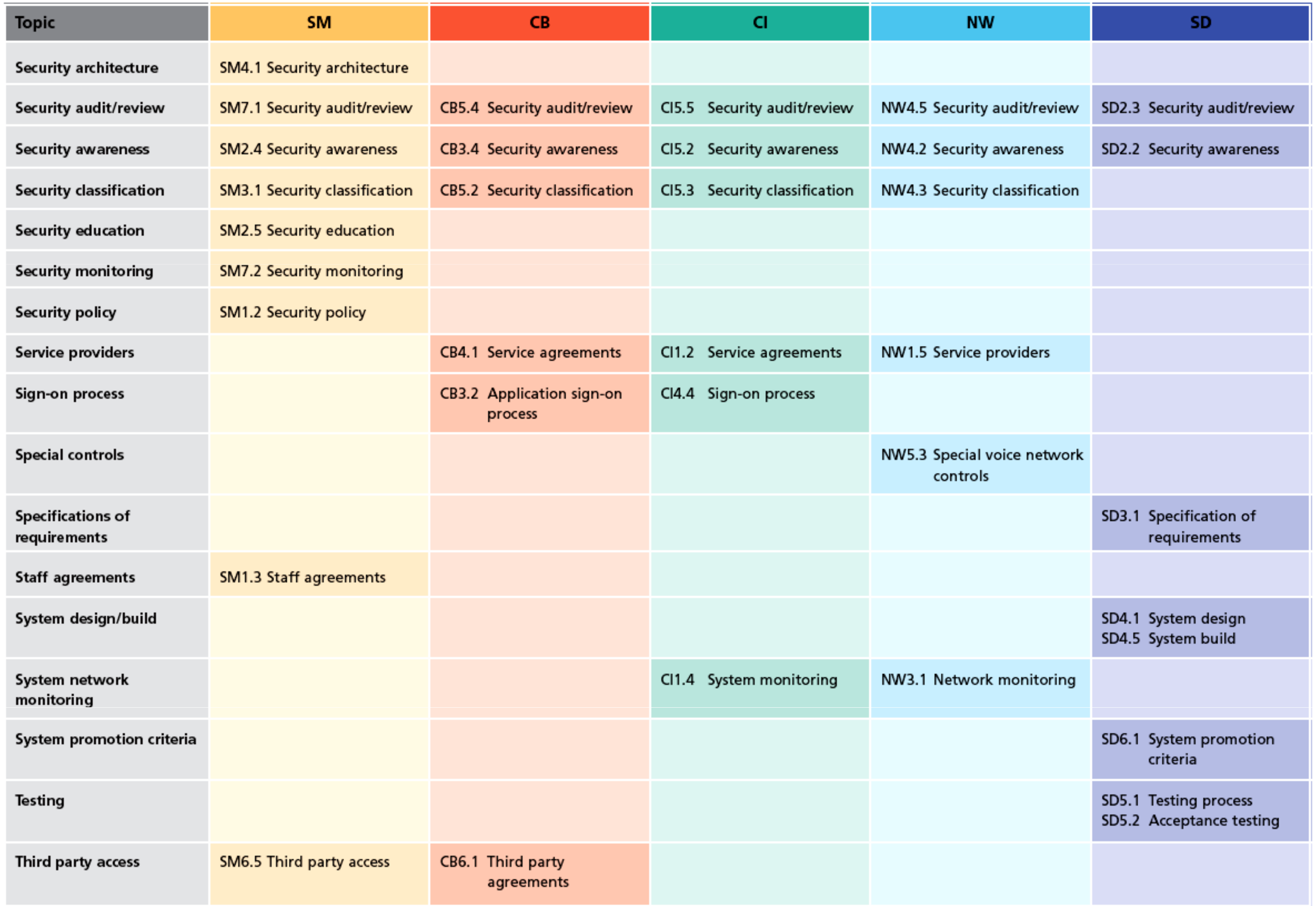
Topic	SM	CB	CI	NW	SD
Emergency fixes			CI3.5 Emergency fixes		
Event logging			CI2.2 Event logging		
External access/ connections		CB4.3 External connections		NW2.3 External access	
Firewalls				NW2.2 Firewalls	
Forensic investigations	SM5.5 Forensic investigations				
General security controls					SD4.3 General security controls
Handling information		CB2.6 Sensitive information	CI3.1 Handling computer media		
Hazard protection			CI2.6 Hazard protection		
Host system configuration			CI2.3 Host system configuration		
Incident management	SM5.4 Emergency response	CB2.4 Incident management	CI3.4 Incident management	NW3.3 Incident management	
Information privacy	SM4.2 Information privacy				
Information security function	SM2.2 Information security function				
Installation and network design			CI2.1 Installation design	NW1.2 Network design	
Instant Messaging	SM 6.8 Instant Messaging				
Installation process					SD6.2 Installation process
Integrity requirements		CB1.2 Integrity requirements			SD3.3 Integrity requirements
Intrusion detection	SM5.3 Intrusion detection				

Info Security Forum Matrix – (4)



Topic	SM	CB	CI	NW	SD
Local security co-ordination	SM2.3 Local security co-ordination	CB5.1 Local security co-ordination	CI5.1 Local security co-ordination	NW4.1 Local security co-ordination	SD2.1 Local security co-ordination
Management commitment	SM1.1 Management commitment SM2.1 High-level control				
Malicious mobile code protection	SM5.2 Malicious mobile code protection				
Network documentation				NW1.4 Network documentation NW5.1 Voice network documentation	
Outsourcing	SM6.7 Outsourcing				
Patch Management	SM 5.6 Patch management		CI3.6 Patch management		
Physical protection	SM4.4 Physical protection		CI2.8 Physical access	NW3.4 Physical security	
Post-implementation review					SD6.3 Post-implementation review
Power supplies			CI2.7 Power supplies		
Public key infrastructure	SM6.2 Public key infrastructure	CB6.3 Public key infrastructure			
Quality assurance					SD1.3 Quality assurance
Remote maintenance				NW3.7 Remote maintenance	
Remote working	SM6.4 Remote working				
Resilience		CB4.2 Resilience	CI2.5 Resilience	NW1.3 Network resilience NW5.2 Resilience of voice networks	
Risk analysis/assessment	SM3.3 Information risk analysis	CB5.3 Information risk analysis	CI5.4 Information risk analysis	NW4.4 Information risk analysis	SD3.5 Information risk assessment
Roles and responsibilities	SM3.2 Ownership	CB2.1 Roles and responsibilities	CI1.1 Roles and responsibilities	NW1.1 Roles and responsibilities	SD1.1 Roles and responsibilities

Info Security Forum Matrix – (5)



Topic	SM	CB	CI	NW	SD
Security architecture	SM4.1 Security architecture				
Security audit/review	SM7.1 Security audit/review	CB5.4 Security audit/review	CI5.5 Security audit/review	NW4.5 Security audit/review	SD2.3 Security audit/review
Security awareness	SM2.4 Security awareness	CB3.4 Security awareness	CI5.2 Security awareness	NW4.2 Security awareness	SD2.2 Security awareness
Security classification	SM3.1 Security classification	CB5.2 Security classification	CI5.3 Security classification	NW4.3 Security classification	
Security education	SM2.5 Security education				
Security monitoring	SM7.2 Security monitoring				
Security policy	SM1.2 Security policy				
Service providers		CB4.1 Service agreements	CI1.2 Service agreements	NW1.5 Service providers	
Sign-on process		CB3.2 Application sign-on process	CI4.4 Sign-on process		
Special controls				NW5.3 Special voice network controls	
Specifications of requirements					SD3.1 Specification of requirements
Staff agreements	SM1.3 Staff agreements				
System design/build					SD4.1 System design SD4.5 System build
System network monitoring			CI1.4 System monitoring	NW3.1 Network monitoring	
System promotion criteria					SD6.1 System promotion criteria
Testing					SD5.1 Testing process SD5.2 Acceptance testing
Third party access	SM6.5 Third party access	CB6.1 Third party agreements			

* Workshop Session 5 *

"Cybersecurity Continuity Planning, Standards and Architectures"

1 – International Standards	2 – ITU Security Standards	3 – ITU: X.805 Architecture
4 – ITU: X1205 CyberSecurity	5 – Others: ISO/IEC & NIST	6 – ISF: Info Security Forum
7 – Practical Implementation	8 – Cyber Continuity: BCP/DR	9 – Next Steps for Jamaica

Practical Standards Implementation

- *Use:* Cybersecurity Standards and Technological Solutions are of great benefit in the establishment of organisations & operational policies
- *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 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!
- *The ITU X800/X1200 Series* of Recommendations provide excellent ICT security frameworks for Jamaican Government and Enterprises, whilst the ISO/IEC 27001/27002 are accepted worldwide for ISMS operations

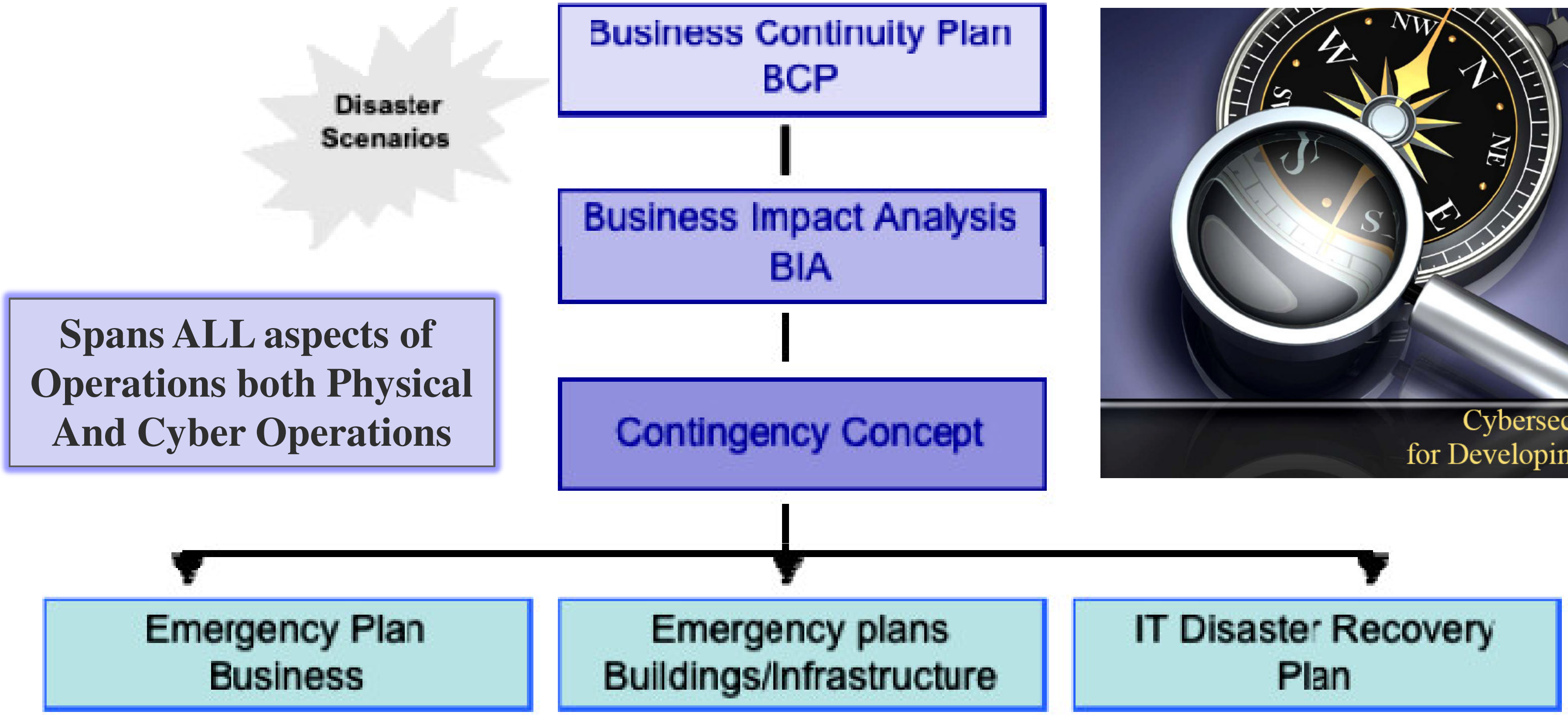
…….Engineering and Managing ICT Operations to International Standards will place a major deterrence upon cybercriminals, hackers & attackers.

* Workshop Session 5 *

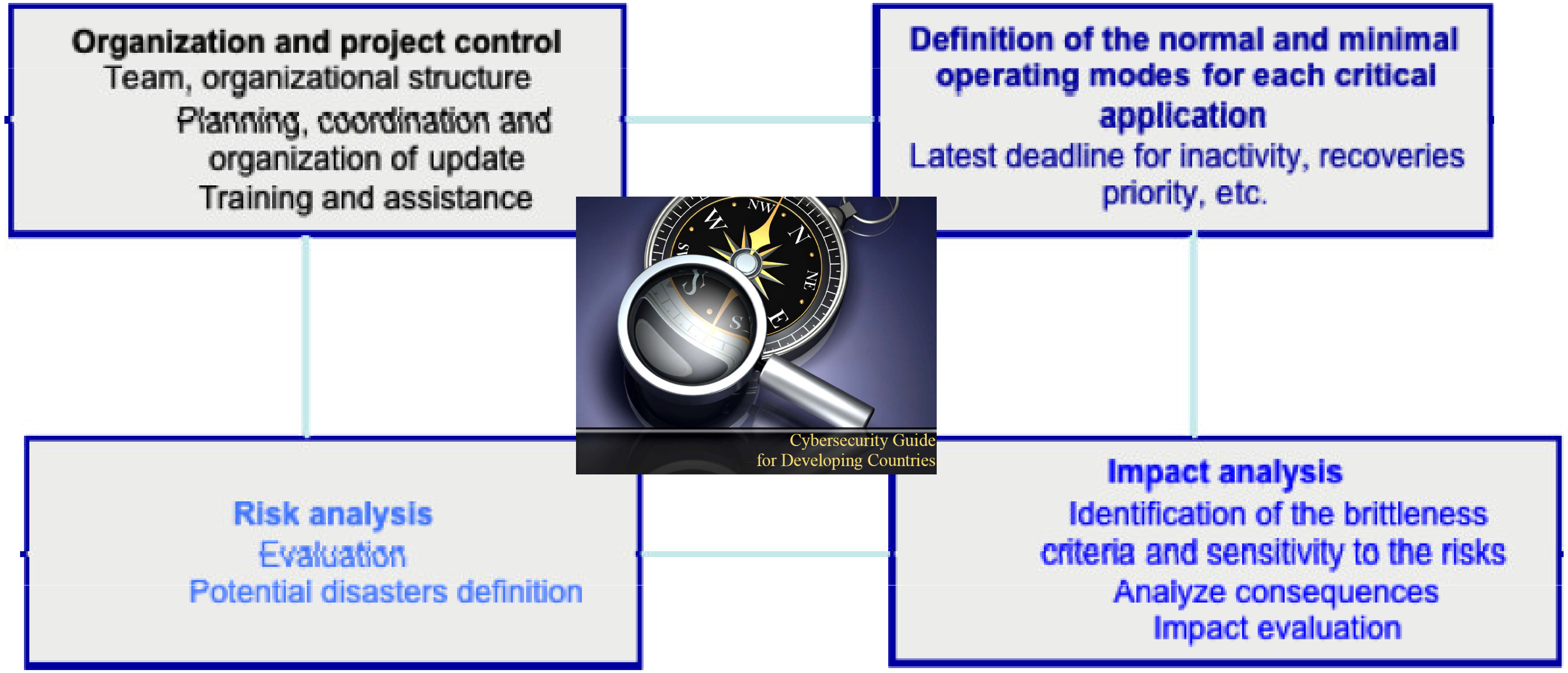
"Cybersecurity Continuity Planning, Standards and Architectures"

1 – International Standards	2 – ITU Security Standards	3 – ITU: X.805 Architecture
4 – ITU: X1205 CyberSecurity	5 – Others: ISO/IEC & NIST	6 – ISF: Info Security Forum
7 – Practical Implementation	8 – Cyber Continuity: BCP/DR	9 – Next Steps for Jamaica

Business Continuity and Disaster Recovery Plans


Disaster Scenarios
Business Continuity Plan BCP
Business Impact Analysis BIA
Contingency Concept
Spans ALL aspects of Operations both Physical And Cyber Operations
Emergency Plan Business
Emergency plans Buildings/Infrastructure
IT Disaster Recovery Plan

Disaster Recovery Planning (DR): Strategic Analysis Process



Organization and project control
Team, organizational structure
Planning, coordination and organization of update
Training and assistance

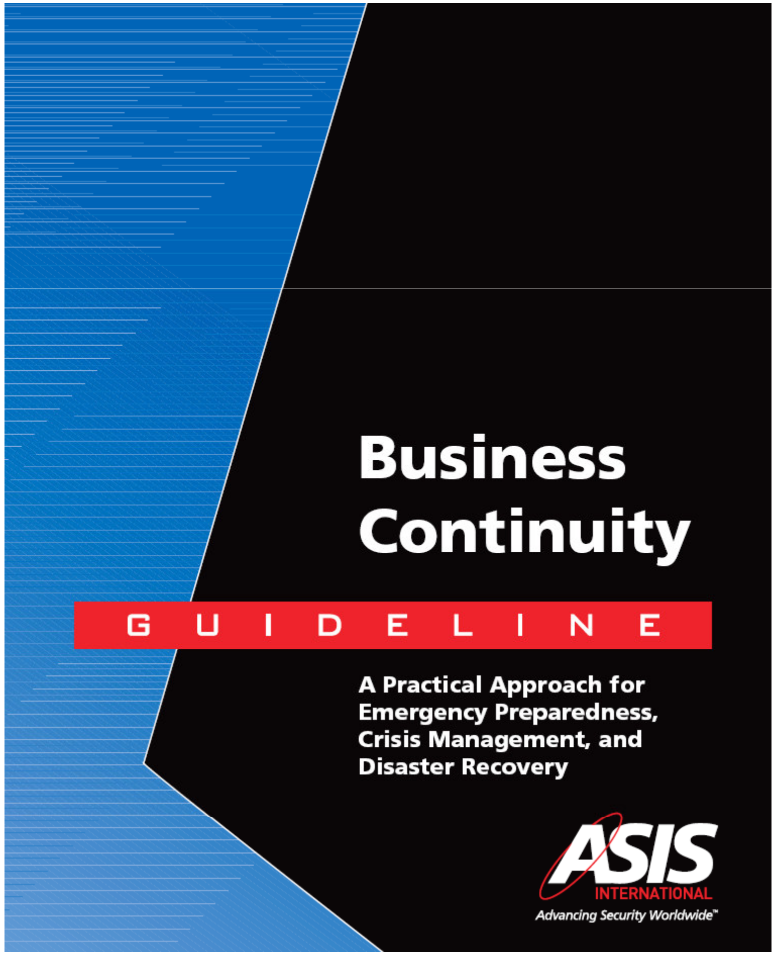
Definition of the normal and minimal operating modes for each critical application
Latest deadline for inactivity, recoveries priority, etc.

Risk analysis
Evaluation
Potential disasters definition

Impact analysis
Identification of the brittleness criteria and sensitivity to the risks
Analyze consequences
Impact evaluation

Figure V.15: Design methodology of a disaster recovery plan (strategic analysis step)

Cyber Continuity & Recovery

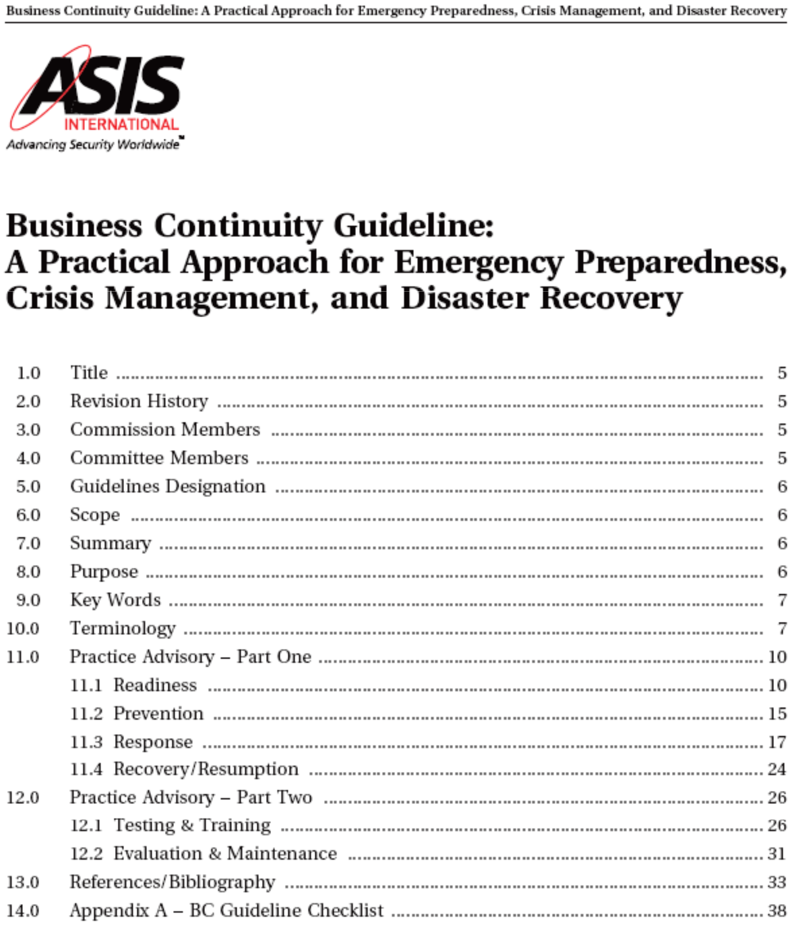


Business Continuity

GUIDELINE

A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery

ASIS INTERNATIONAL
Advancing Security Worldwide™



Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery

ASIS INTERNATIONAL
Advancing Security Worldwide™

Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery

1.0 Title 5
2.0 Revision History 5
3.0 Commission Members 5
4.0 Committee Members 5
5.0 Guidelines Designation 6
6.0 Scope 6
7.0 Summary 6
8.0 Purpose 6
9.0 Key Words 7
10.0 Terminology 7
11.0 Practice Advisory – Part One 10
11.1 Readiness 10
11.2 Prevention 15
11.3 Response 17
11.4 Recovery/Resumption 24
12.0 Practice Advisory – Part Two 26
12.1 Testing & Training 26
12.2 Evaluation & Maintenance 31
13.0 References/Bibliography 33
14.0 Appendix A – BC Guideline Checklist 38

Useful General Guidelines on Business Continuity and Disaster Recovery from ASIS

* Workshop Session 5 *

"Cybersecurity Continuity Planning, Standards and Architectures"

1 – International Standards	2 – ITU Security Standards	3 – ITU: X.805 Architecture
4 – ITU: X1205 CyberSecurity	5 – Others: ISO/IEC & NIST	6 – ISF: Info Security Forum
7 – Practical Implementation	8 – Cyber Continuity: BCP/DR	9 – Next Steps for Jamaica

Next Action Steps for Jamaica

- ***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 Jamaican ICT systems and Operational Procedures will have a significant impact on cybercrime, & reduce the risk of attacks on critical national infrastructure

* ITU Workshop Overview*

“Cybersecurity Technologies, Standards & Operations”

S1-Thurs: 9:30-11:00 “The International Cybercrime and Cybersecurity Challenge”	S2–Thurs:11:30-13:00 “Integration Cyber-Technological Solutions for the 21stC Web2.0 World”	S3-Thurs:14:00-15:30 Group Session: “Securing Critical Computing and Network Facilities”	S4-Thurs:16:00-17:30 Group Session: “Group Discussion: Securing Critical Computing and Network Facilities”
S5 - Fri: 9:30–11:00 “Cybersecurity Continuity Planning, Standards and Architectures”	S6 – Fri: 11:30–13:00 “Organising a National Crime Unit and CERT/CSIRT”	S7 – Fri: 14:00-15:30 Group Session: “Designing Practical Cybercrime Solutions – Critical Sectors”	S7 – Fri: 16:00-17:30 Group Session” “Group Discussion: Designing Practical Cybercrime Solutions – Critical Sectors”

* Workshop Session 6 *

Organising a National Cybercrime Unit (NCU) and National CERT/CSIRT

1–Special Cyber Organisations	2 – CERT/CSIRT Organisation	3 – CERT/CSIRT Alert Centre
4 – CERT/CSIRT: Roll-Out Plan	5 – National Cybercrime Unit	6 – National Cybercrime Unit
7 – ITU: IMPACT Programme	8 – ITU: IMPACT Programme	9 –"Best Practice" for Jamaica

* Workshop Session 6 *

Organising a National Cybercrime Unit (NCU) and National CERT/CSIRT

1–Special Cyber Organisations	2 – CERT/CSIRT Organisation	3 – CERT/CSIRT Alert Centre
4 – CERT/CSIRT: Roll-Out Plan	5 – National Cybercrime Unit	6 – National Cybercrime Unit
7 – ITU: IMPACT Programme	8 – ITU: IMPACT Programme	9 –“Best Practice” for Jamaica

Special Cybersecurity Technical Organisations

- Effective national and enterprise cybersecurity requires the implementation of professionally staffed technical organisations
- In this session we'll consider the cyersecurity organisations and associated technical skills for:
  - CERT/CSIRT: Computer Emergency Response Team – *We'll explore the steps required to establish and manage a National or Enterprise CERT. We will use the CMU (Carnegie Mellon University), and ENISA (European Network & Information Security Agency) Guidelines as the foundations for our technical and management analysis*
  - NCU/eCrime Unit: National Cybercrime Unit – *We'll use the UK National eCrime Unit as an example of "Best Practice" for the organisation, including the process for cybercrime investigation, evidence collection and the skills for Digital Forensics*
  - Global IMPACT Centre: International Multi-Lateral Partnership against Cyber Threats - *This is a unique organisation is an alliance with several major global players including the ITU and Interpol. We'll present some of the programmes that may be relevant to the Jamaican Government, major Institutions and Commercial Enterprises*

* Workshop Session 6 *

Organising a National Cybercrime Unit (NCU) and National CERT/CSIRT

1–Special Cyber Organisations	2 – CERT/CSIRT Organisation	3 – CERT/CSIRT Alert Centre
4 – CERT/CSIRT: Roll-Out Plan	5 – National Cybercrime Unit	6 – National Cybercrime Unit
7 – ITU: IMPACT Programme	8 – ITU: IMPACT Programme	9 –"Best Practice" for Jamaica

CERT/CSIRT Organisations

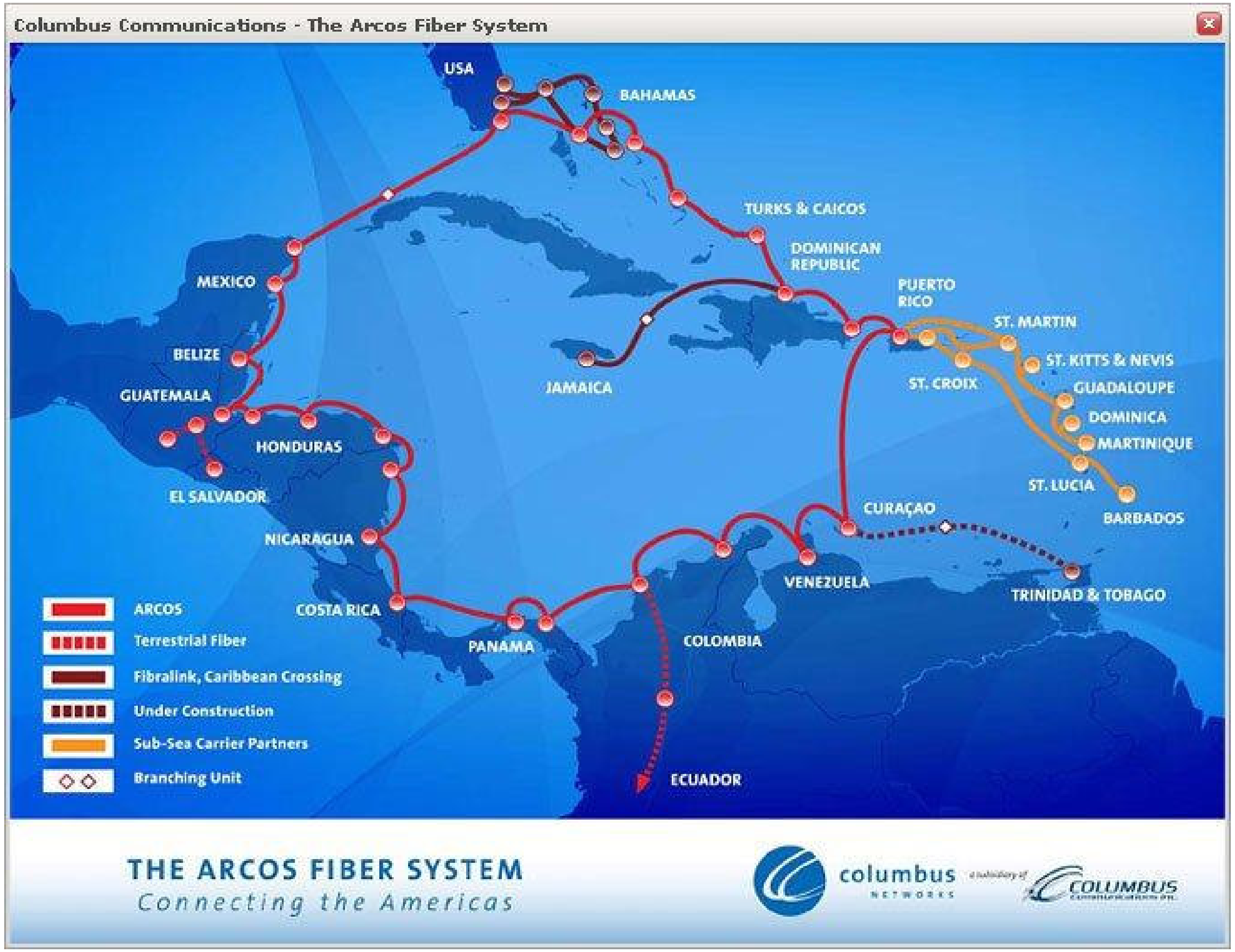
- *Benefits:* Every national government, and major multi-site enterprise should consider the economic benefits of establishing a CERT/CSIRT.

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

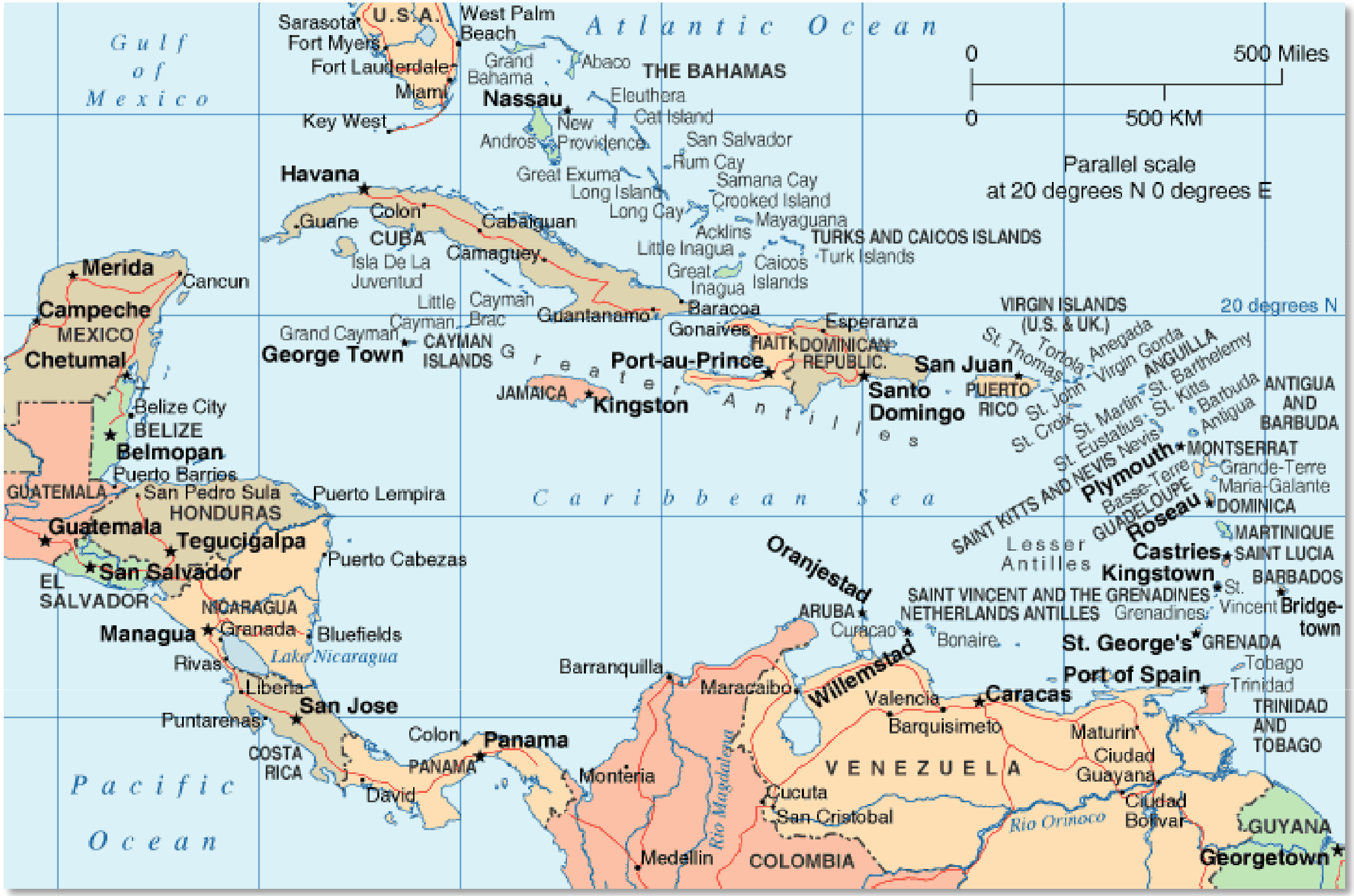
- *CERT.org:* Carnegie Mellon University formed the 1st National CERT under contract from the US Government, and now runs www.CERT.org as a global partnership of national and regional CERTs.

- *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.

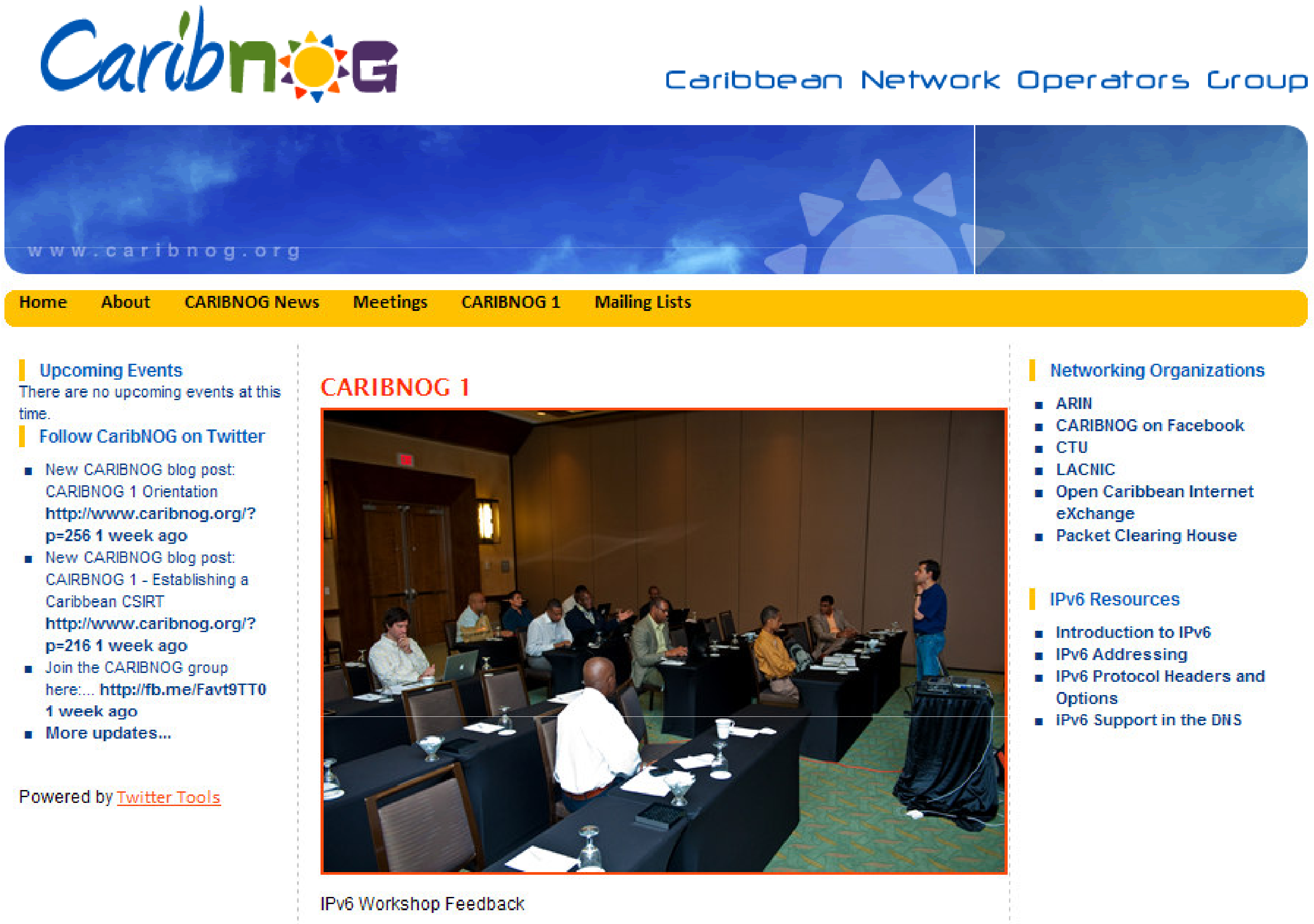
Caribbean Connectivity



Securing the Caribbean in Cyberspace



Regional Caribbean Network Organisations



Caribbean Network Operators Group

www.caribnog.org

Home About CARIBNOG News Meetings CARIBNOG 1 Mailing Lists

Upcoming Events

There are no upcoming events at this time.

Follow CaribNOG on Twitter

- New CARIBNOG blog post: CARIBNOG 1 Orientation http://www.caribnog.org/?p=256 1 week ago
- New CARIBNOG blog post: CAIRBNOG 1 - Establishing a Caribbean CSIRT http://www.caribnog.org/?p=216 1 week ago
- Join the CARIBNOG group here:... http://fb.me/Favt9TT0 1 week ago
- More updates...

Powered by Twitter Tools

CARIBNOG 1

IPv6 Workshop Feedback

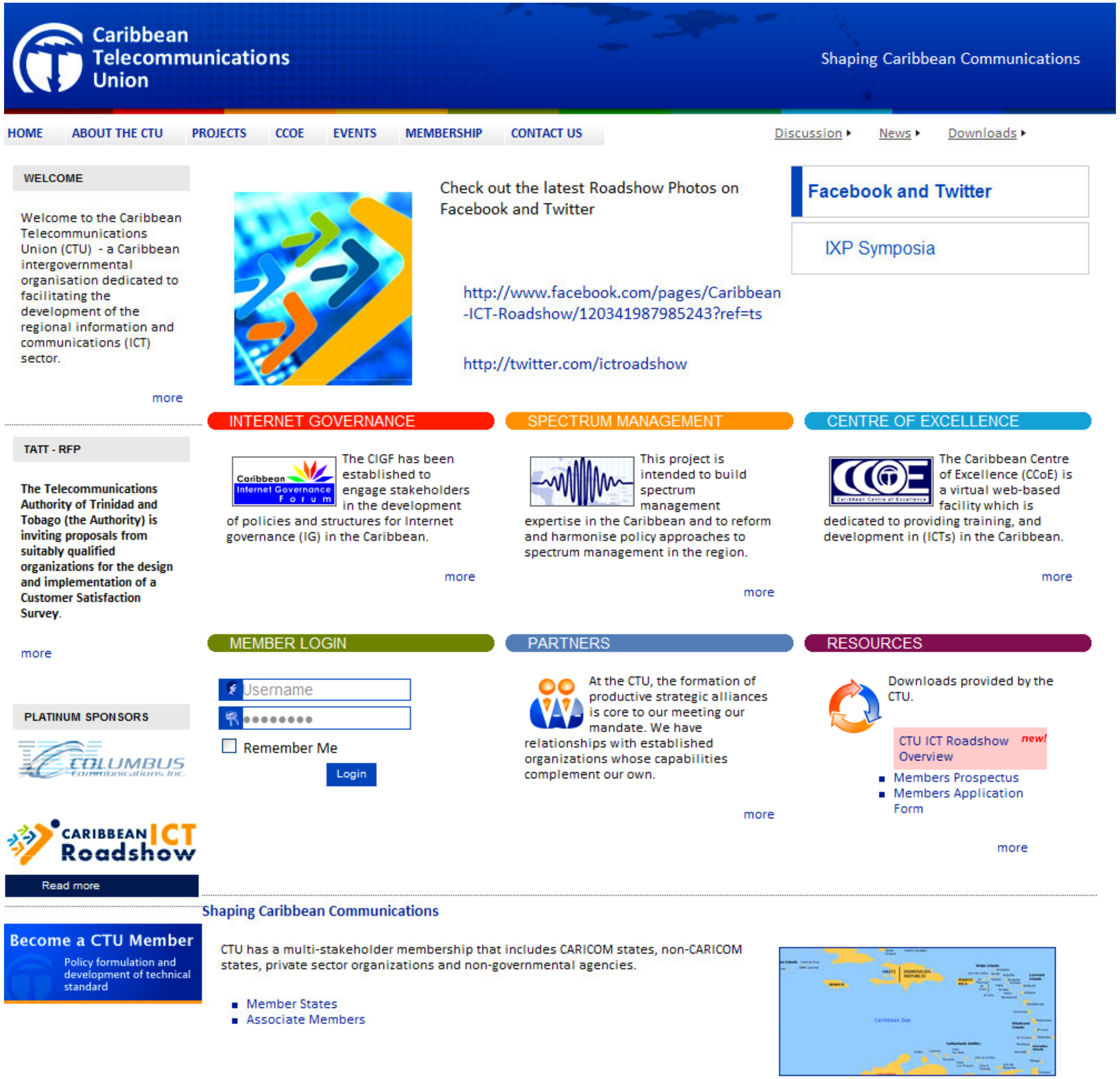
Networking Organizations

- ARIN
- CARIBNOG on Facebook
- CTU
- LACNIC
- Open Caribbean Internet eXchange
- Packet Clearing House

IPv6 Resources

- Introduction to IPv6
- IPv6 Addressing
- IPv6 Protocol Headers and Options
- IPv6 Support in the DNS

Caribbean Telecommunications Union



Caribbean Telecommunications Union

Shaping Caribbean Communications

HOME | ABOUT THE CTU | PROJECTS | CCOE | EVENTS | MEMBERSHIP | CONTACT US

Discussion ▸ News ▸ Downloads ▸

WELCOME

Welcome to the Caribbean Telecommunications Union (CTU) - a Caribbean intergovernmental organisation dedicated to facilitating the development of the regional information and communications (ICT) sector.

more

Check out the latest Roadshow Photos on Facebook and Twitter

http://www.facebook.com/pages/Caribbean-ICT-Roadshow/120341987985243?ref=ts

http://twitter.com/ictroadshow

Facebook and Twitter

IXP Symposia

TATT - RFP

The Telecommunications Authority of Trinidad and Tobago (the Authority) is inviting proposals from suitably qualified organizations for the design and implementation of a Customer Satisfaction Survey.

more

INTERNET GOVERNANCE

The CIGF has been established to engage stakeholders in the development of policies and structures for Internet governance (IG) in the Caribbean.

more

SPECTRUM MANAGEMENT

This project is intended to build spectrum management expertise in the Caribbean and to reform and harmonise policy approaches to spectrum management in the region.

more

CENTRE OF EXCELLENCE

The Caribbean Centre of Excellence (CCoE) is a virtual web-based facility which is dedicated to providing training, and development in (ICTs) in the Caribbean.

more

PLATINUM SPONSORS

MEMBER LOGIN

Username

●●●●●●●●

□ Remember Me

Login

PARTNERS

At the CTU, the formation of productive strategic alliances is core to our meeting our mandate. We have relationships with established organizations whose capabilities complement our own.

more

RESOURCES

Downloads provided by the CTU.

CTU ICT Roadshow Overview *new!*

- Members Prospectus
- Members Application Form

more

CARIBBEAN ICT Roadshow

Read more

Shaping Caribbean Communications

Become a CTU Member

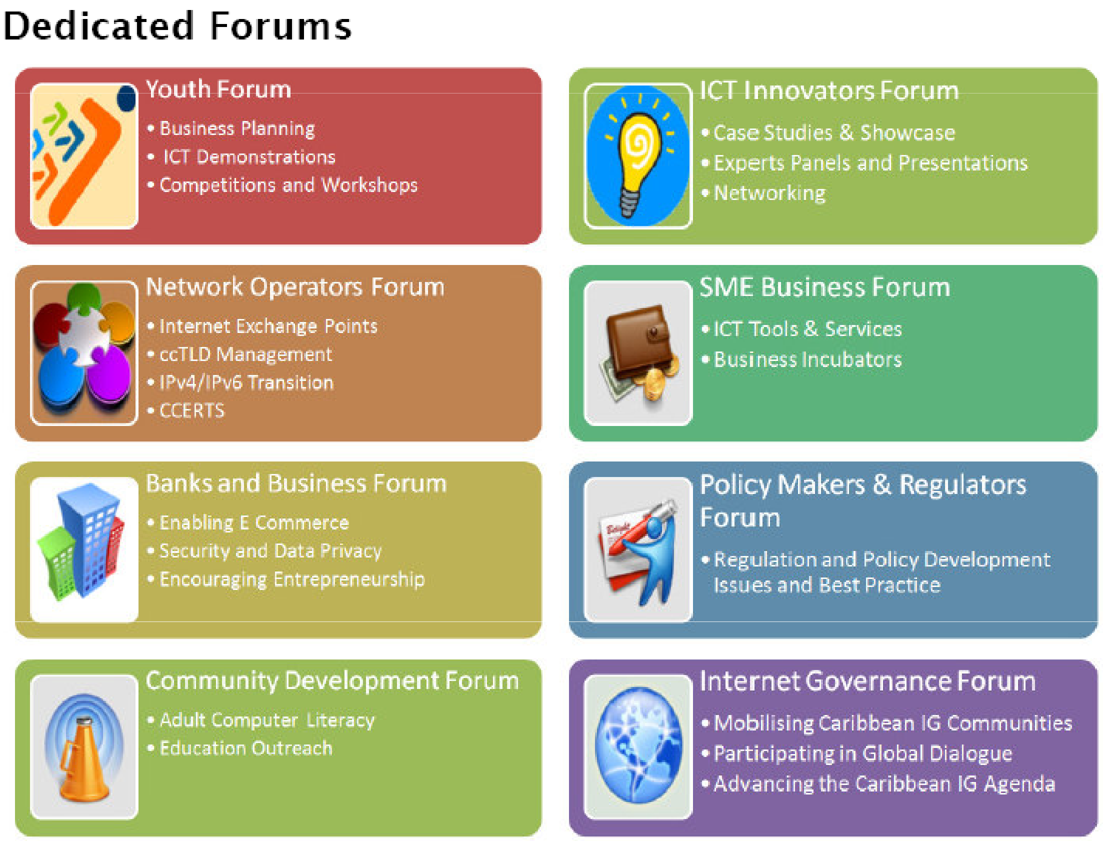
Policy formulation and development of technical standard

CTU has a multi-stakeholder membership that includes CARICOM states, non-CARICOM states, private sector organizations and non-governmental agencies.

- Member States
- Associate Members

CTU: Caribbean ICT Roadshow (CIRS)

CARIBBEAN ICT Roadshow



Dedicated Forums

Youth Forum
- Business Planning
- ICT Demonstrations
- Competitions and Workshops

ICT Innovators Forum
- Case Studies & Showcase
- Experts Panels and Presentations
- Networking

Network Operators Forum
- Internet Exchange Points
- ccTLD Management
- IPv4/IPv6 Transition
- CCERTS

SME Business Forum
- ICT Tools & Services
- Business Incubators

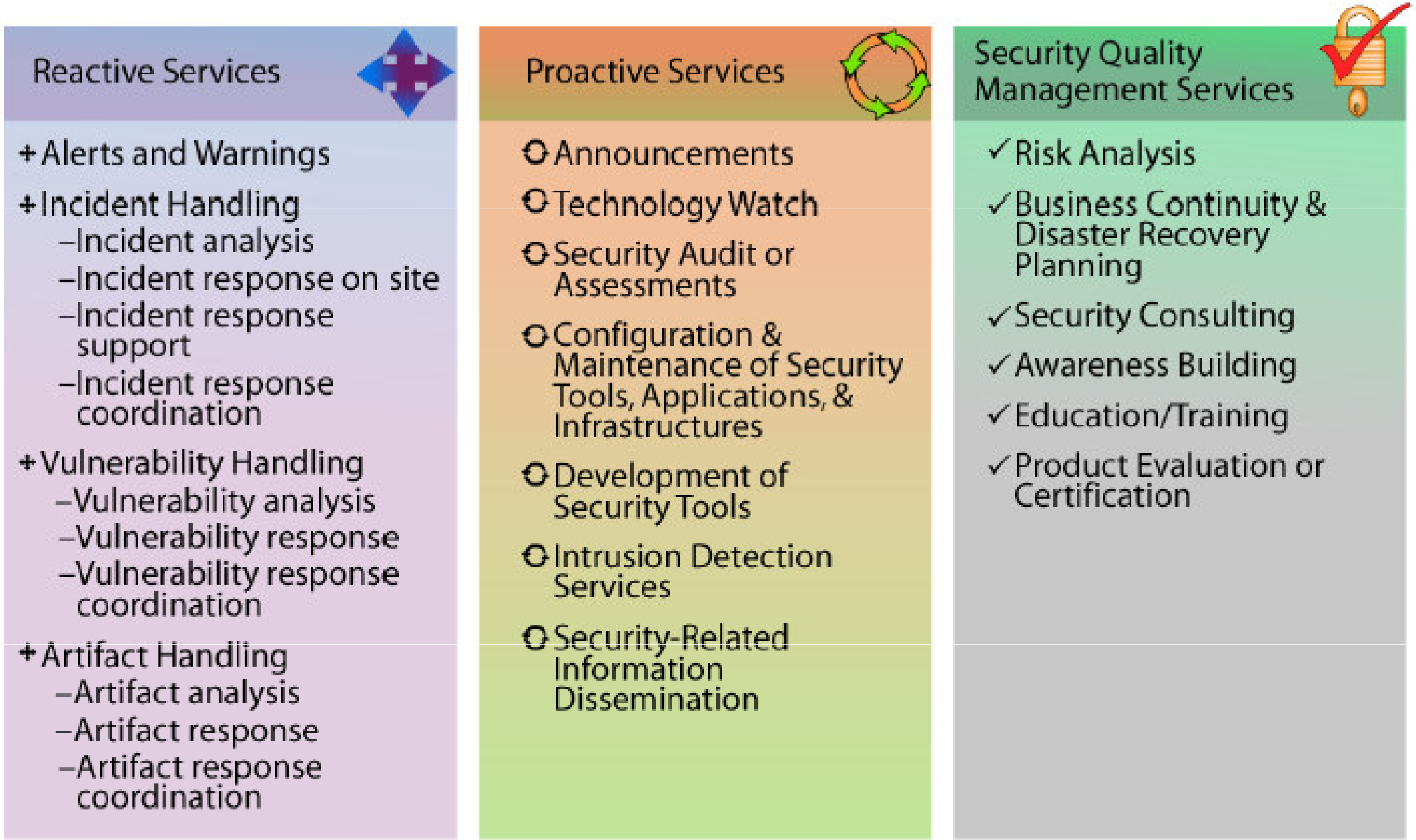
Banks and Business Forum
- Enabling E Commerce
- Security and Data Privacy
- Encouraging Entrepreneurship

Policy Makers & Regulators Forum
- Regulation and Policy Development Issues and Best Practice

Community Development Forum
- Adult Computer Literacy
- Education Outreach

Internet Governance Forum
- Mobilising Caribbean IG Communities
- Participating in Global Dialogue
- Advancing the Caribbean IG Agenda

CERT/CSIRT Services



Reactive Services

- Alerts and Warnings
- Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- Artifact Handling
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

Proactive Services

- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services

- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

* Workshop Session 6 *

Organising a National Cybercrime Unit (NCU) and National CERT/CSIRT

1–Special Cyber Organisations	2 – CERT/CSIRT Organisation	3 – CERT/CSIRT Alert Centre
4 – CERT/CSIRT: Roll-Out Plan	5 – National Cybercrime Unit	6 – National Cybercrime Unit
7 – ITU: IMPACT Programme	8 – ITU: IMPACT Programme	9 –"Best Practice" for Jamaica

CERT/CSIRT 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

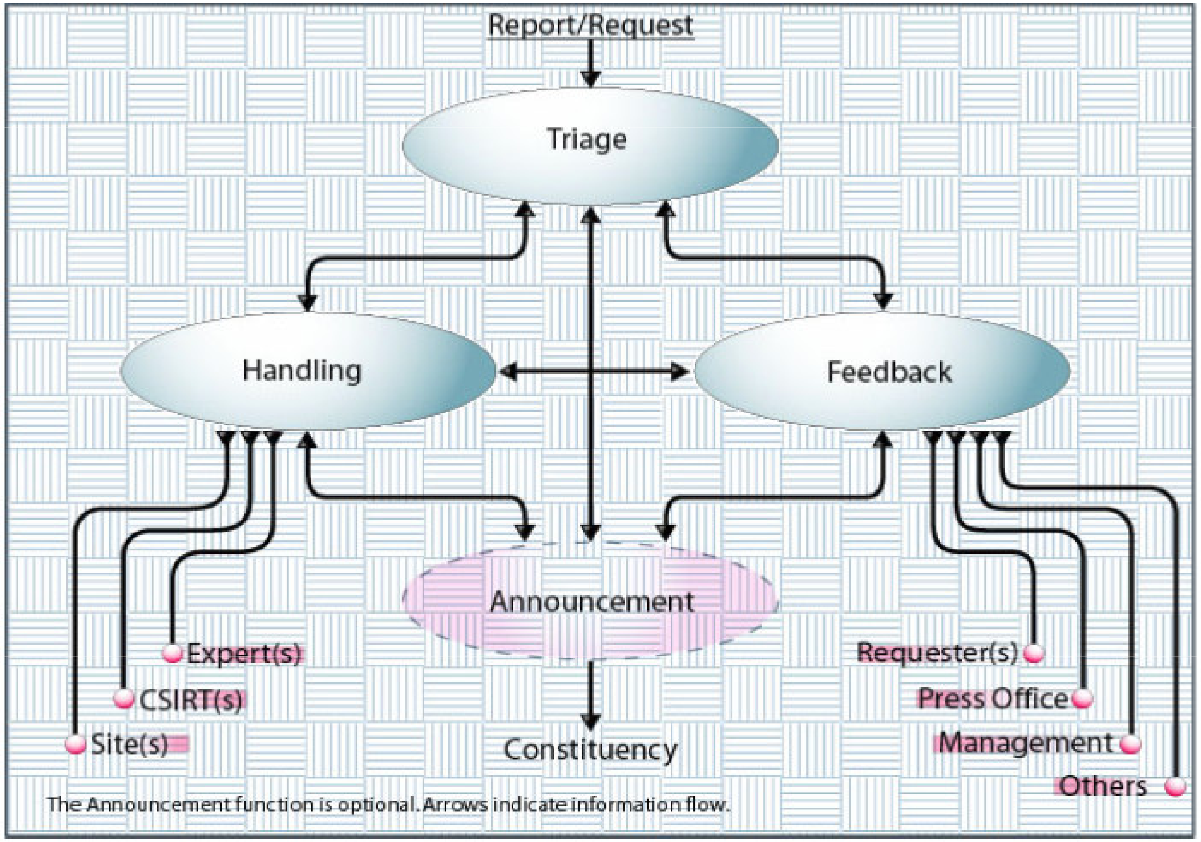
- *Risk:* Once an incident is classified the CERT will need to assign staff responsibility to assess the event risk and potential impact & damage

- *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

…………The following slide shows this incident process flow in more detail…

CERT/CSIRT: Incident Handling Service Functions



The Announcement function is optional. Arrows indicate information flow.

CSIRT – Information Process Flow

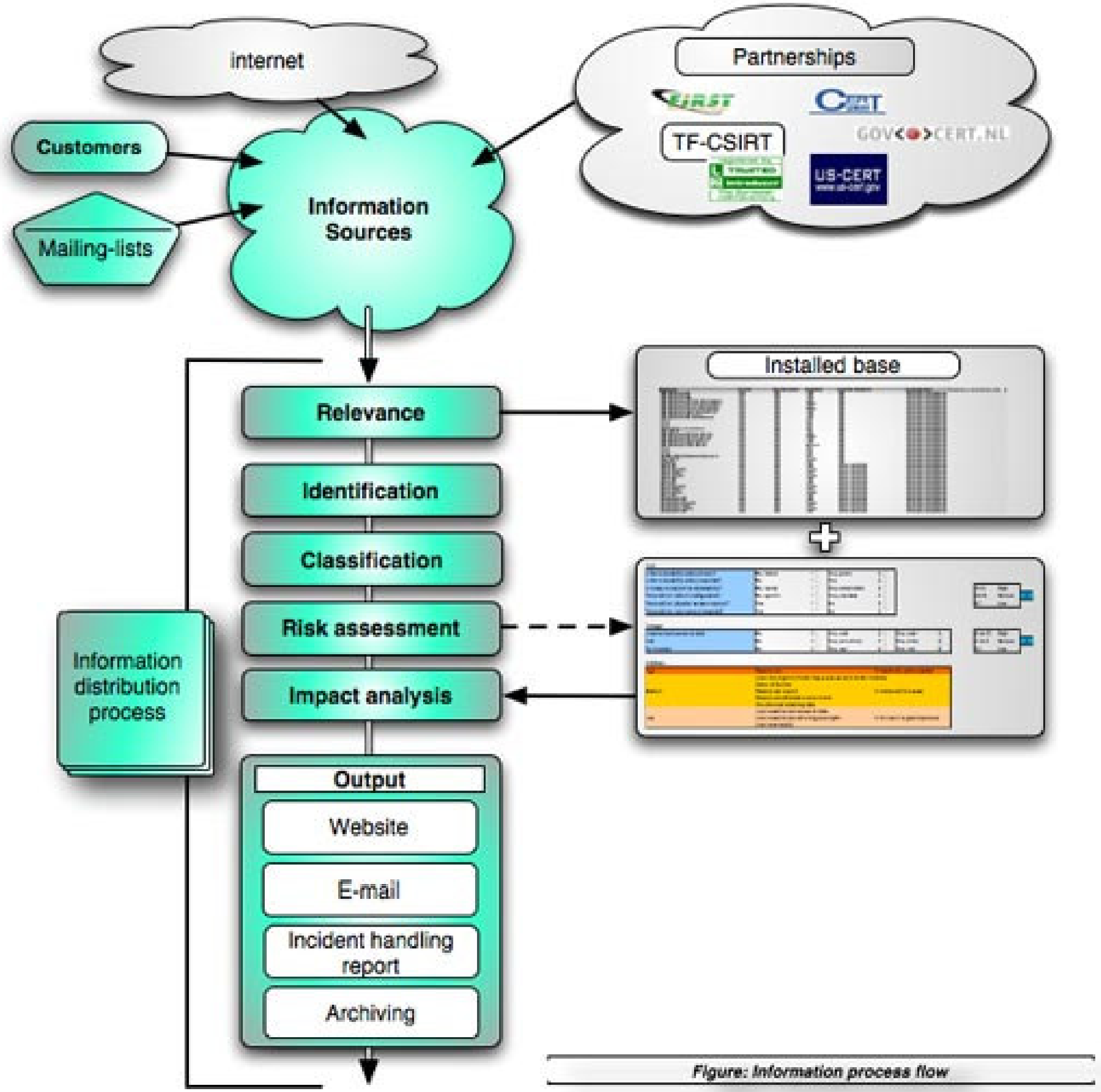


Figure: Information process flow

ITU Centres of Excellence Network for the Caribbean Region
Cybersecurity Technologies, Standards & Operations
16-17 September, Kingston, Jamaica

Incident Handling Process Flow

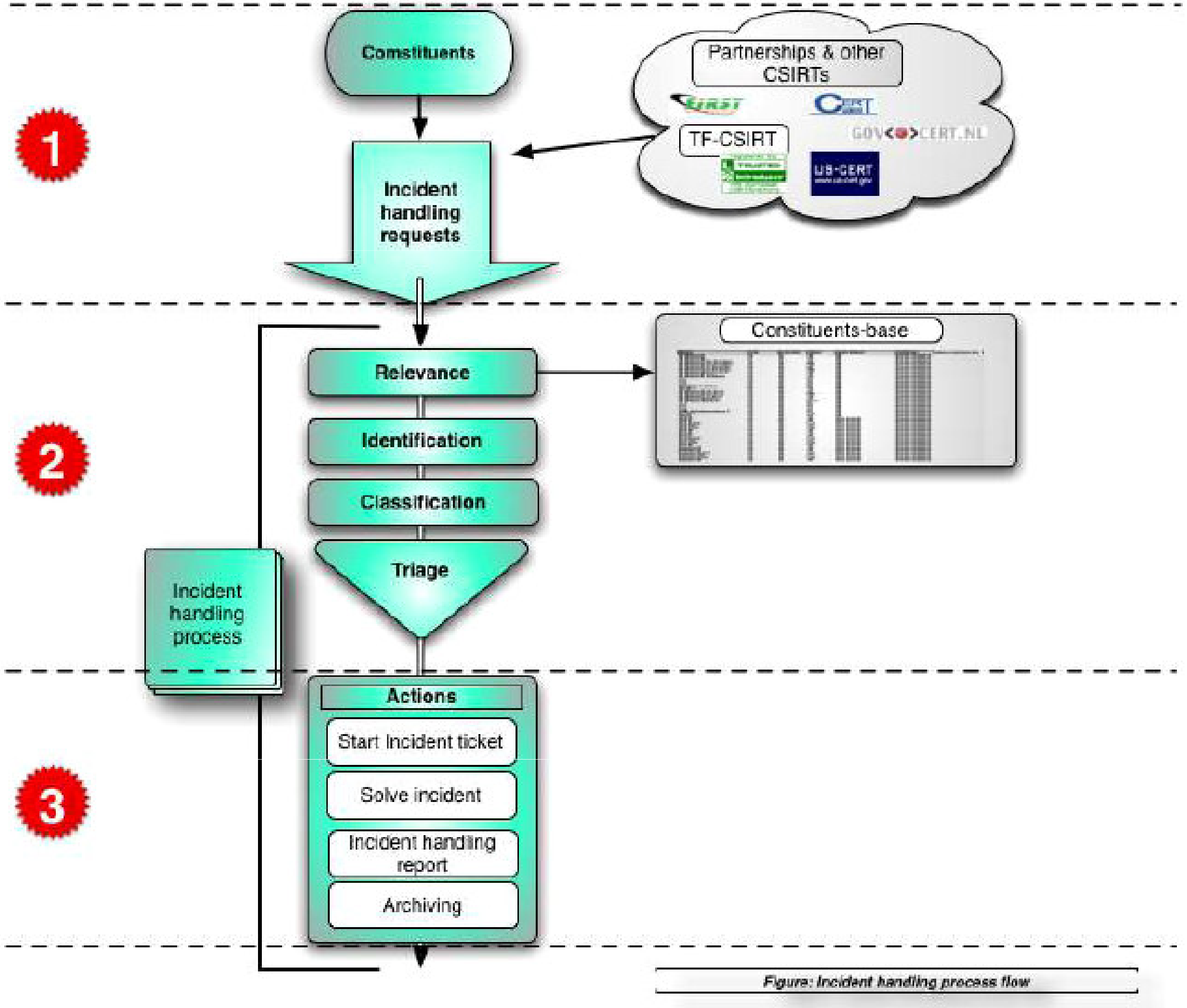


Figure: Incident handling process flow

Cyber-Incident Depth Analysis

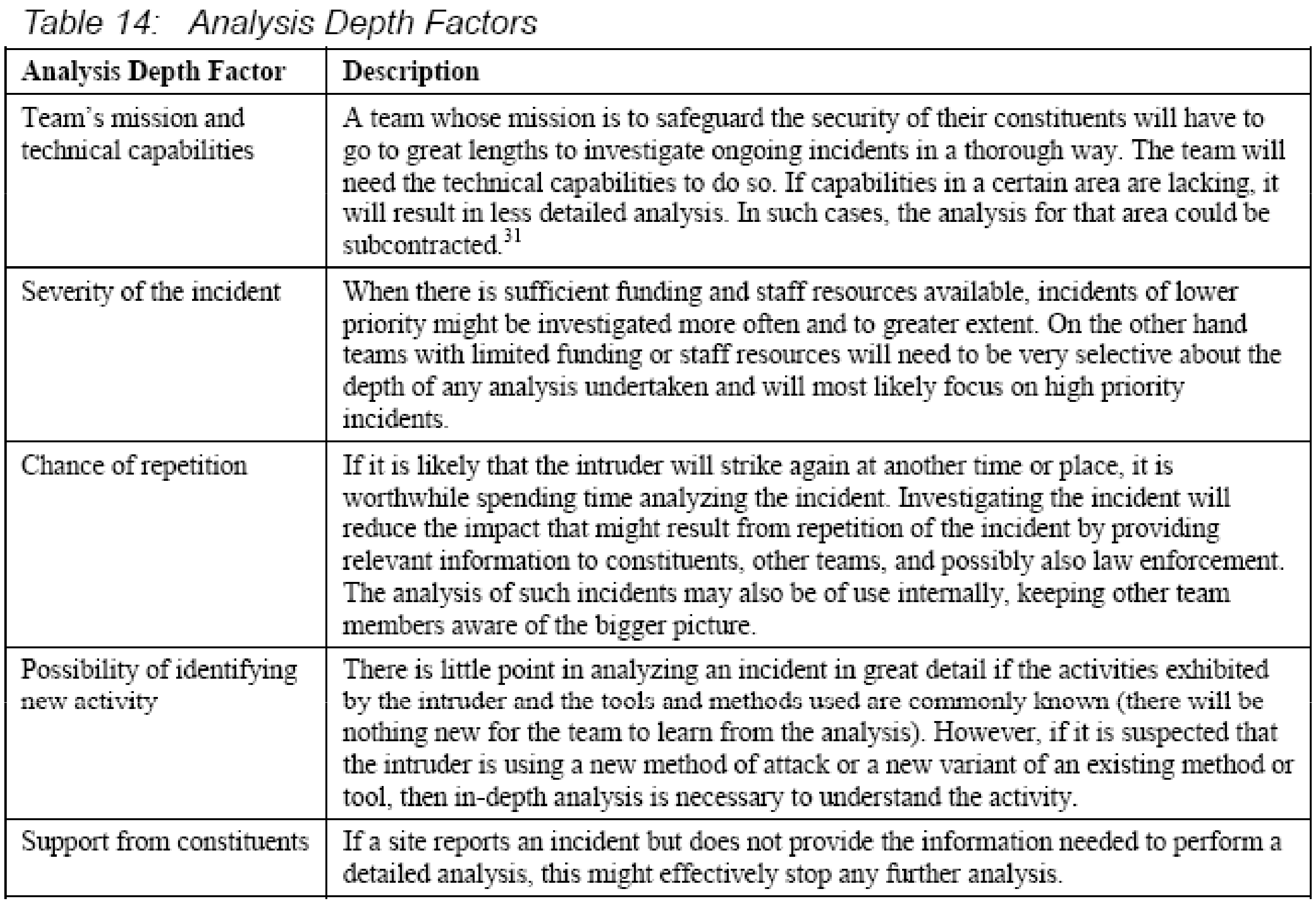
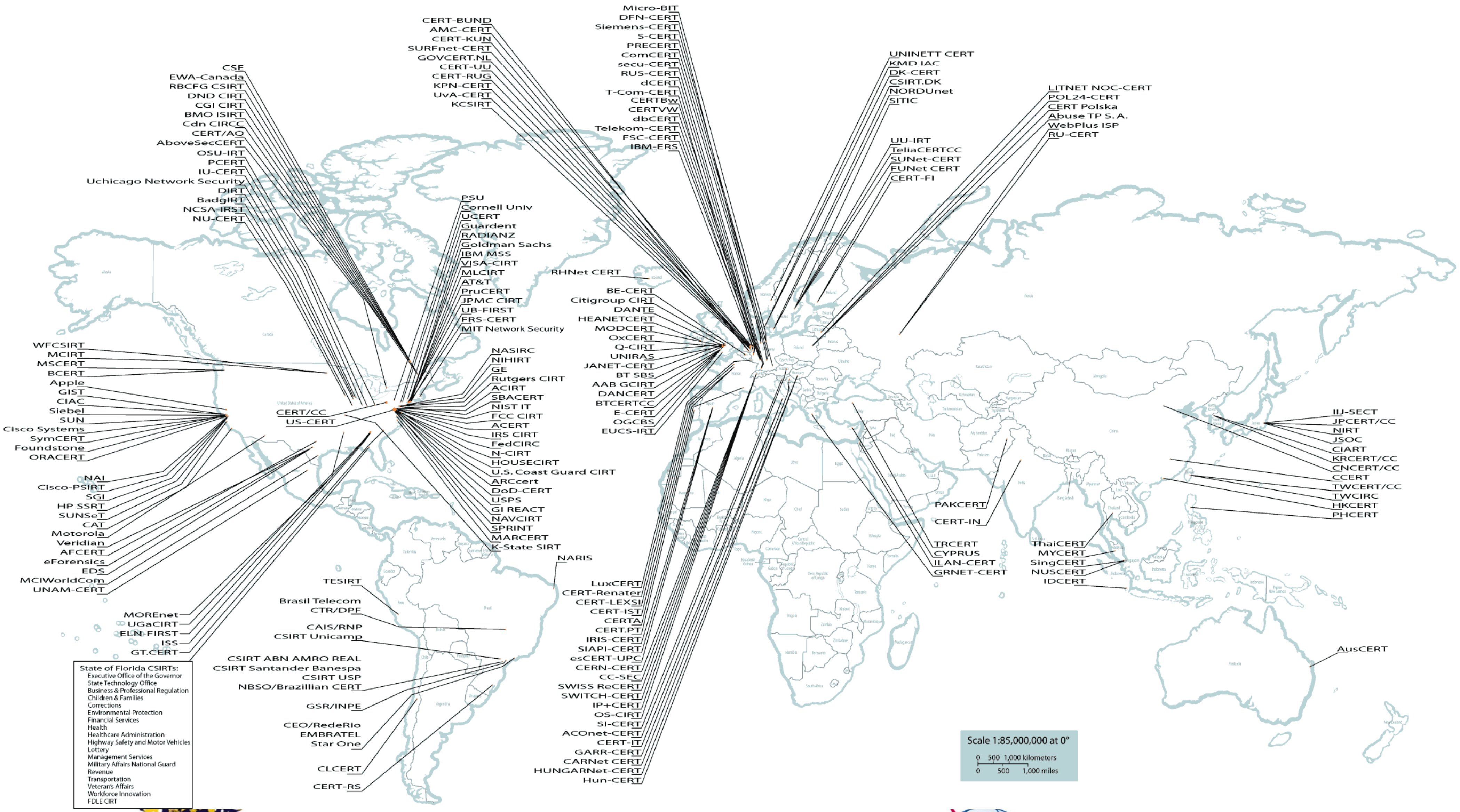


Table 14: Analysis Depth Factors

Analysis Depth Factor	Description
Team's mission and technical capabilities	A team whose mission is to safeguard the security of their constituents will have to go to great lengths to investigate ongoing incidents in a thorough way. The team will need the technical capabilities to do so. If capabilities in a certain area are lacking, it will result in less detailed analysis. In such cases, the analysis for that area could be subcontracted.[31]
Severity of the incident	When there is sufficient funding and staff resources available, incidents of lower priority might be investigated more often and to greater extent. On the other hand teams with limited funding or staff resources will need to be very selective about the depth of any analysis undertaken and will most likely focus on high priority incidents.
Chance of repetition	If it is likely that the intruder will strike again at another time or place, it is worthwhile spending time analyzing the incident. Investigating the incident will reduce the impact that might result from repetition of the incident by providing relevant information to constituents, other teams, and possibly also law enforcement. The analysis of such incidents may also be of use internally, keeping other team members aware of the bigger picture.
Possibility of identifying new activity	There is little point in analyzing an incident in great detail if the activities exhibited by the intruder and the tools and methods used are commonly known (there will be nothing new for the team to learn from the analysis). However, if it is suspected that the intruder is using a new method of attack or a new variant of an existing method or tool, then in-depth analysis is necessary to understand the activity.
Support from constituents	If a site reports an incident but does not provide the information needed to perform a detailed analysis, this might effectively stop any further analysis.

Incident Response Teams Around the World

International cooperation speeds response to Internet security breaches.

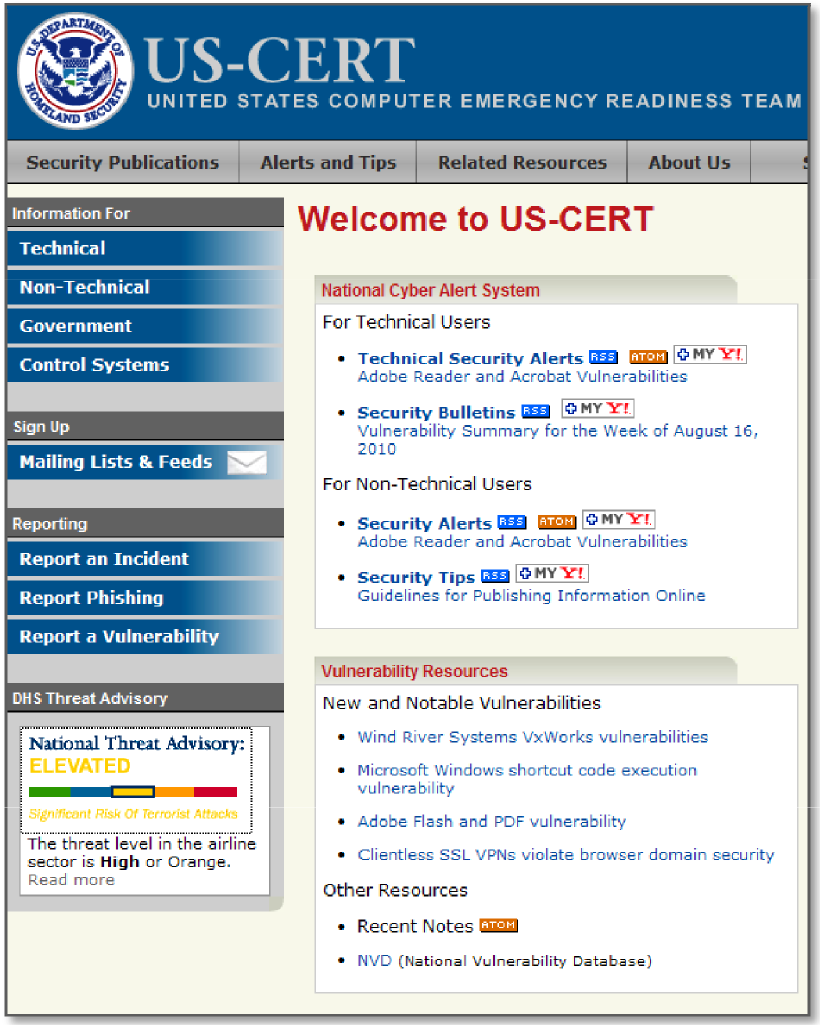


University of Technology, Jamaica

ITU Centres of Excellence Network for the Caribbean Region
Cybersecurity Technologies, Standards & Operations
16-17 September, Kingston, Jamaica

International Telecommunication Union
Committed to connecting the world

US and Asia-Pacific CERTs



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Information For

- Technical
- Non-Technical
- Government
- Control Systems

Sign Up

- Mailing Lists & Feeds

Reporting

- Report an Incident
- Report Phishing
- Report a Vulnerability

DHS Threat Advisory

National Threat Advisory: ELEVATED

Significant Risk Of Terrorist Attacks

The threat level in the airline sector is **High** or Orange.
Read more

Welcome to US-CERT

National Cyber Alert System

For Technical Users

- **Technical Security Alerts** RSS ATOM MY Y!
  Adobe Reader and Acrobat Vulnerabilities
- **Security Bulletins** RSS MY Y!
  Vulnerability Summary for the Week of August 16, 2010

For Non-Technical Users

- **Security Alerts** RSS ATOM MY Y!
  Adobe Reader and Acrobat Vulnerabilities
- **Security Tips** RSS MY Y!
  Guidelines for Publishing Information Online

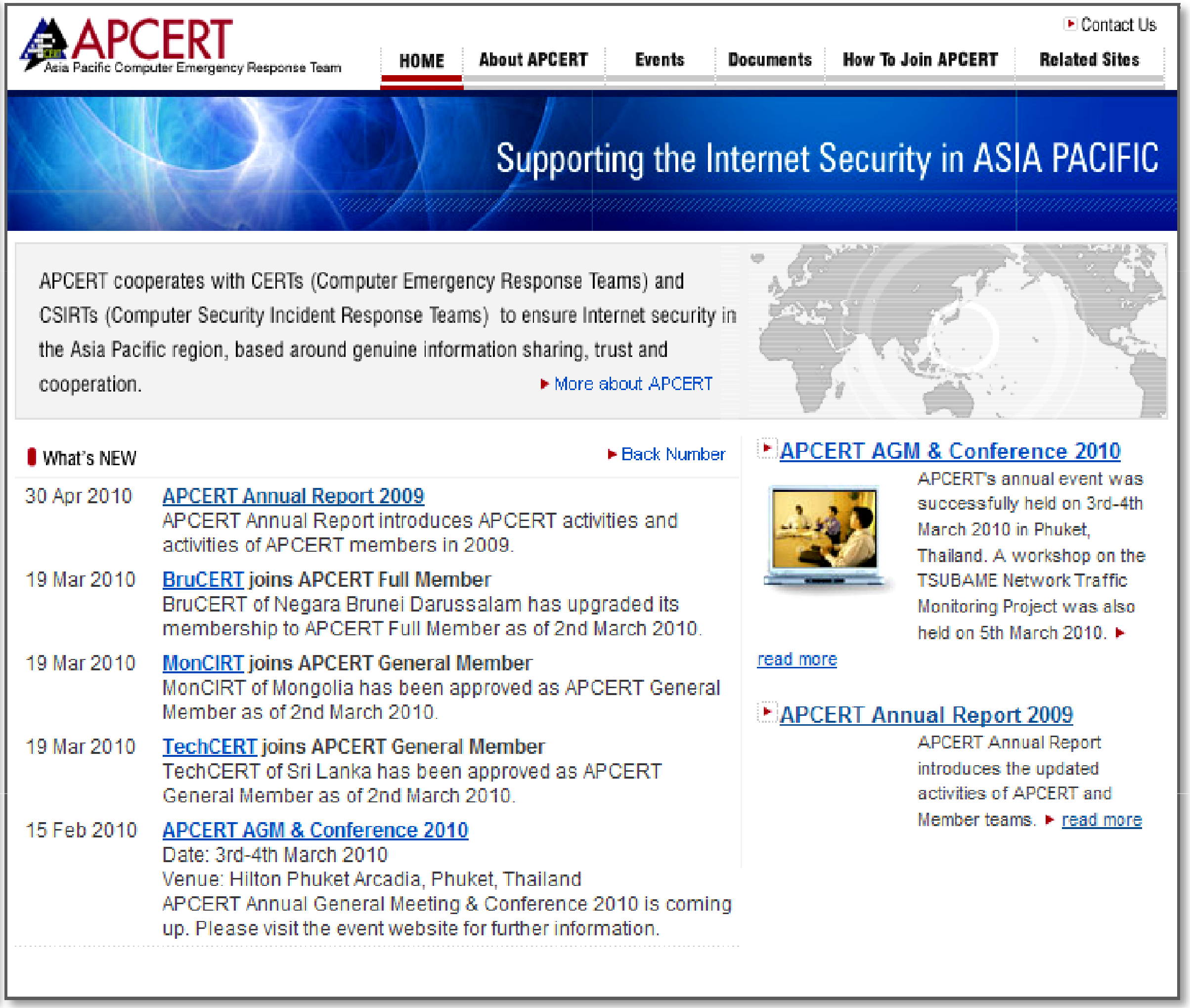
Vulnerability Resources

New and Notable Vulnerabilities

- Wind River Systems VxWorks vulnerabilities
- Microsoft Windows shortcut code execution vulnerability
- Adobe Flash and PDF vulnerability
- Clientless SSL VPNs violate browser domain security

Other Resources

- Recent Notes ATOM
- NVD (National Vulnerability Database)



APCERT
Asia Pacific Computer Emergency Response Team

APCERT cooperates with CERTs (Computer Emergency Response Teams) and CSIRTs (Computer Security Incident Response Teams) to ensure Internet security in the Asia Pacific region, based around genuine information sharing, trust and cooperation. ▸ More about APCERT

What's NEW ▸ Back Number

30 Apr 2010	APCERT Annual Report 2009 APCERT Annual Report introduces APCERT activities and activities of APCERT members in 2009.
19 Mar 2010	BruCERT joins APCERT Full Member BruCERT of Negara Brunei Darussalam has upgraded its membership to APCERT Full Member as of 2nd March 2010.
19 Mar 2010	MonCIRT joins APCERT General Member MonCIRT of Mongolia has been approved as APCERT General Member as of 2nd March 2010.
19 Mar 2010	TechCERT joins APCERT General Member TechCERT of Sri Lanka has been approved as APCERT General Member as of 2nd March 2010.
15 Feb 2010	APCERT AGM & Conference 2010 Date: 3rd-4th March 2010 Venue: Hilton Phuket Arcadia, Phuket, Thailand APCERT Annual General Meeting & Conference 2010 is coming up. Please visit the event website for further information.

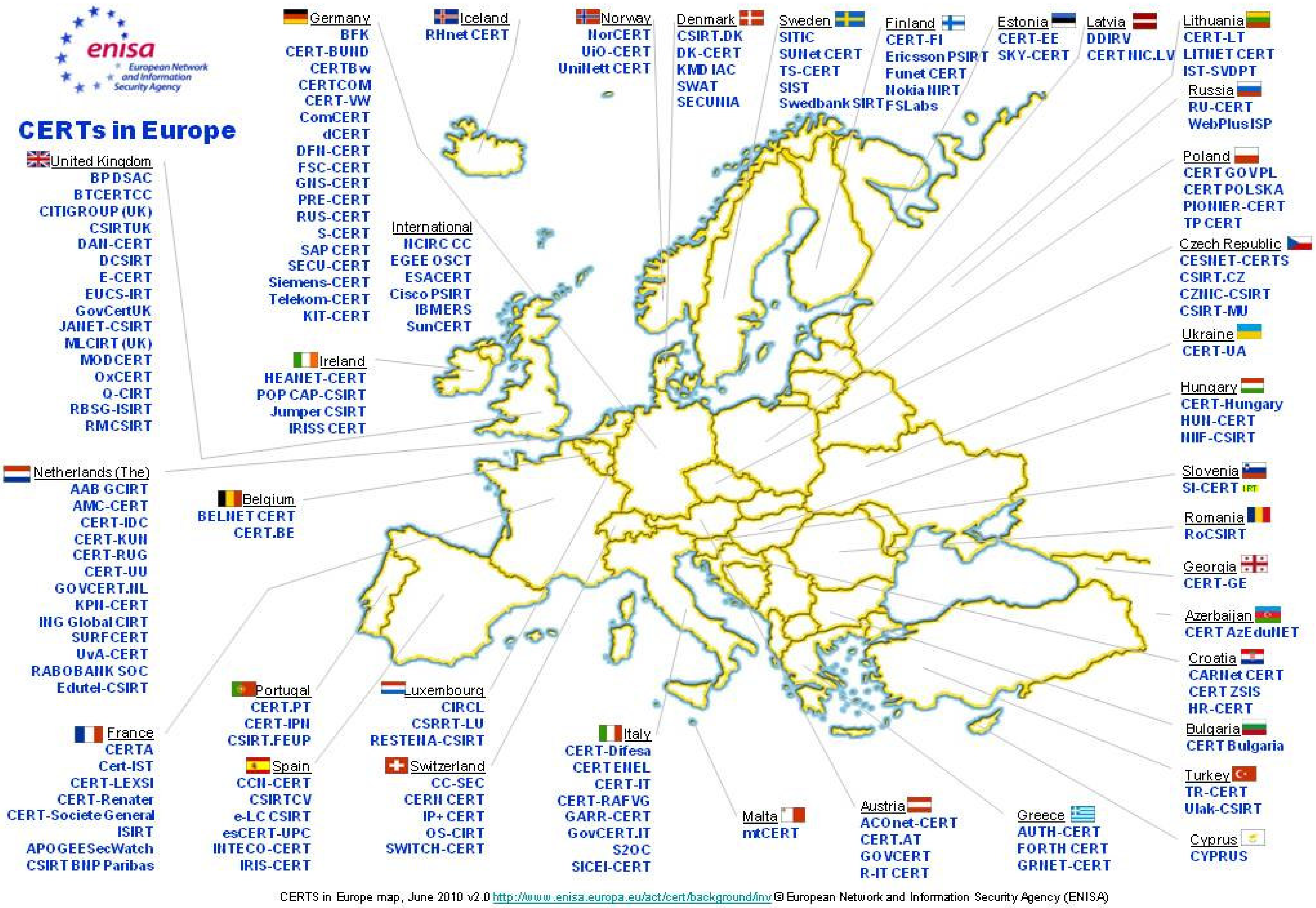
APCERT AGM & Conference 2010

APCERT's annual event was successfully held on 3rd-4th March 2010 in Phuket, Thailand. A workshop on the TSUBAME Network Traffic Monitoring Project was also held on 5th March 2010. ▸
read more

APCERT Annual Report 2009

APCERT Annual Report introduces the updated activities of APCERT and Member teams. ▸ read more

ENISA: European CERT Network



enisa European Network and Information Security Agency

CERTs in Europe

United Kingdom
BP DSAC
BTCERTCC
CITIGROUP (UK)
CSIRTUK
DAN-CERT
DCSIRT
E-CERT
EUCS-IRT
GovCertUK
JANET-CSIRT
MLCIRT (UK)
MODCERT
OxCERT
Q-CIRT
RBSG-ISIRT
RMCSIRT

Netherlands (The)
AAB GCIRT
AMC-CERT
CERT-IDC
CERT-KUN
CERT-RUG
CERT-UU
GOVCERT.NL
KPN-CERT
ING Global CIRT
SURFCERT
UvA-CERT
RABOBANK SOC
Edutel-CSIRT

France
CERTA
Cert-IST
CERT-LEXSI
CERT-Renater
CERT-Societe General
ISIRT
APOGEESecWatch
CSIRT BNP Paribas

Germany
BFK
CERT-BUND
CERTBw
CERTCOM
CERT-VW
ComCERT
dCERT
DFN-CERT
FSC-CERT
GNS-CERT
PRE-CERT
RUS-CERT
S-CERT
SAP CERT
SECU-CERT
Siemens-CERT
Telekom-CERT
KIT-CERT

Ireland
HEANET-CERT
POP CAP-CSIRT
Jumper CSIRT
IRISS CERT

Belgium
BELNET CERT
CERT.BE

Portugal
CERT.PT
CERT-IPN
CSIRT.FEUP

Spain
CCN-CERT
CSIRTCV
e-LC CSIRT
esCERT-UPC
INTECO-CERT
IRIS-CERT

Iceland
RHnet CERT

International
NCIRC CC
EGEE OSCT
ESACERT
Cisco PSIRT
IBMERS
SunCERT

Luxembourg
CIRCL
CSRRT-LU
RESTENA-CSIRT

Switzerland
CC-SEC
CERN CERT
IP+ CERT
OS-CIRT
SWITCH-CERT

Norway
NorCERT
UiO-CERT
UniNett CERT

Italy
CERT-Difesa
CERT ENEL
CERT-IT
CERT-RAFVG
GARR-CERT
GovCERT.IT
S2OC
SICEI-CERT

Denmark
CSIRT.DK
DK-CERT
KMD IAC
SWAT
SECUNIA

Malta
mtCERT

Sweden
SITIC
SUNet CERT
TS-CERT
SIST
Swedbank SIRT

Austria
ACOnet-CERT
CERT.AT
GOVCERT
R-IT CERT

Finland
CERT-FI
Ericsson PSIRT
Funet CERT
Nokia NIRT
FSLabs

Estonia
CERT-EE
SKY-CERT

Greece
AUTH-CERT
FORTH CERT
GRNET-CERT

Latvia
DDIRV
CERT NIC.LV

Lithuania
CERT-LT
LITNET CERT
IST-SVDPT

Russia
RU-CERT
WebPlusISP

Poland
CERT GOVPL
CERT POLSKA
PIONIER-CERT
TP CERT

Czech Republic
CESNET-CERTS
CSIRT.CZ
CZNIC-CSIRT
CSIRT-MU

Ukraine
CERT-UA

Hungary
CERT-Hungary
HUN-CERT
NIIF-CSIRT

Slovenia
SI-CERT IRT

Romania
RoCSIRT

Georgia
CERT-GE

Azerbaijan
CERT AzEduNET

Croatia
CARNet CERT
CERT ZSIS
HR-CERT

Bulgaria
CERT Bulgaria

Turkey
TR-CERT
Ulak-CSIRT

Cyprus
CYPRUS

CERTS in Europe map, June 2010 v2.0 http://www.enisa.europa.eu/act/cert/background/inv © European Network and Information Security Agency (ENISA)

* Workshop Session 6 *

Organising a National Cybercrime Unit (NCU) and National CERT/CSIRT

1–Special Cyber Organisations	2 – CERT/CSIRT Organisation	3 – CERT/CSIRT Alert Centre
4 – CERT/CSIRT: Roll-Out Plan	5 – National Cybercrime Unit	6 – National Cybercrime Unit
7 – ITU: IMPACT Programme	8 – ITU: IMPACT Programme	9 –"Best Practice" for Jamaica

CERT/CSIRT Roll-Out Action Plan

- Jamaican Government and Business may upgrade their CERT/CSIRT capability using the excellent on-line guidebooks from CMU & 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

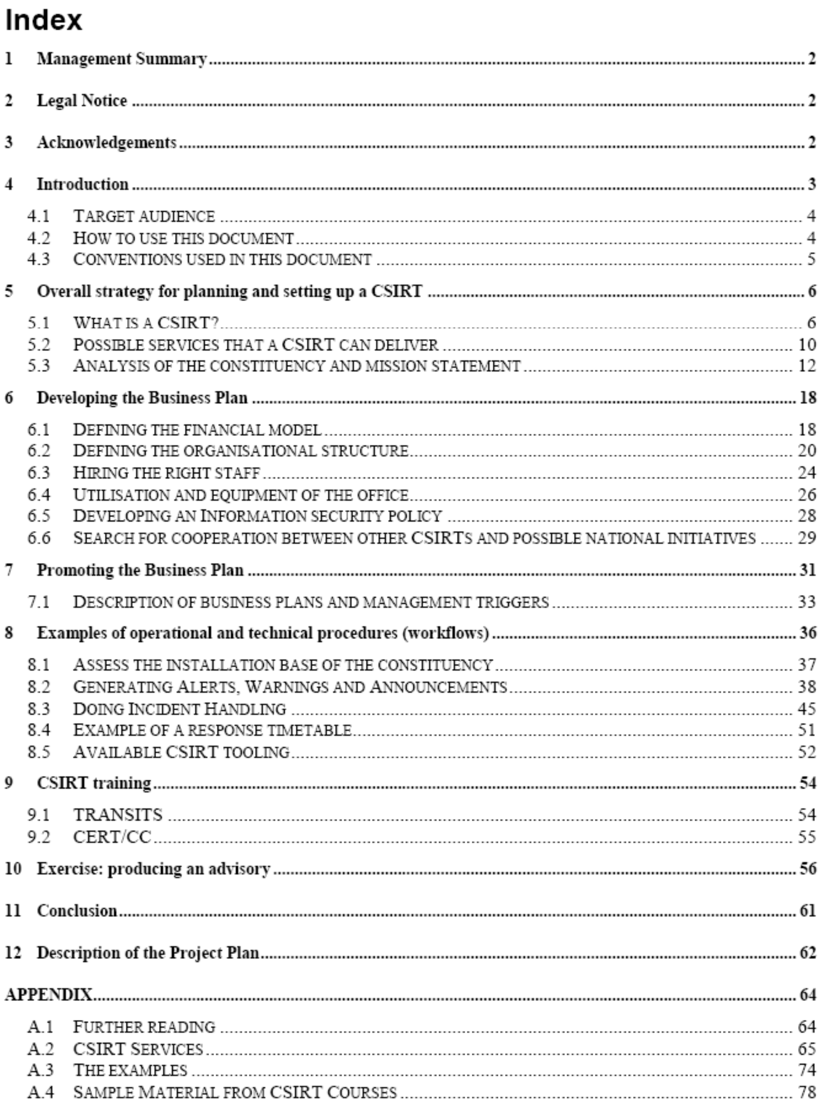
- CERTs will need to continuously evolve, adapt and be trained to respond to new cyberthreats and potential attacks, and will to undergo annual compliance audits

ENISA: CSIRT Guidebook

A STEP-BY-STEP APPROACH ON HOW TO SET UP A CSIRT

Including examples and a checklist in form of a project plan

Deliverable WP2006/5.1(CERT-D1/D2)



Index

1 Management Summary 2

2 Legal Notice 2

3 Acknowledgements 2

4 Introduction 3

4.1 TARGET AUDIENCE 4
4.2 HOW TO USE THIS DOCUMENT 4
4.3 CONVENTIONS USED IN THIS DOCUMENT 5

5 Overall strategy for planning and setting up a CSIRT 6

5.1 WHAT IS A CSIRT? 6
5.2 POSSIBLE SERVICES THAT A CSIRT CAN DELIVER 10
5.3 ANALYSIS OF THE CONSTITUENCY AND MISSION STATEMENT 12

6 Developing the Business Plan 18

6.1 DEFINING THE FINANCIAL MODEL 18
6.2 DEFINING THE ORGANISATIONAL STRUCTURE 20
6.3 HIRING THE RIGHT STAFF 24
6.4 UTILISATION AND EQUIPMENT OF THE OFFICE 26
6.5 DEVELOPING AN INFORMATION SECURITY POLICY 28
6.6 SEARCH FOR COOPERATION BETWEEN OTHER CSIRTS AND POSSIBLE NATIONAL INITIATIVES 29

7 Promoting the Business Plan 31

7.1 DESCRIPTION OF BUSINESS PLANS AND MANAGEMENT TRIGGERS 33

8 Examples of operational and technical procedures (workflows) 36

8.1 ASSESS THE INSTALLATION BASE OF THE CONSTITUENCY 37
8.2 GENERATING ALERTS, WARNINGS AND ANNOUNCEMENTS 38
8.3 DOING INCIDENT HANDLING 45
8.4 EXAMPLE OF A RESPONSE TIMETABLE 51
8.5 AVAILABLE CSIRT TOOLING 52

9 CSIRT training 54

9.1 TRANSITS 54
9.2 CERT/CC 55

10 Exercise: producing an advisory 56

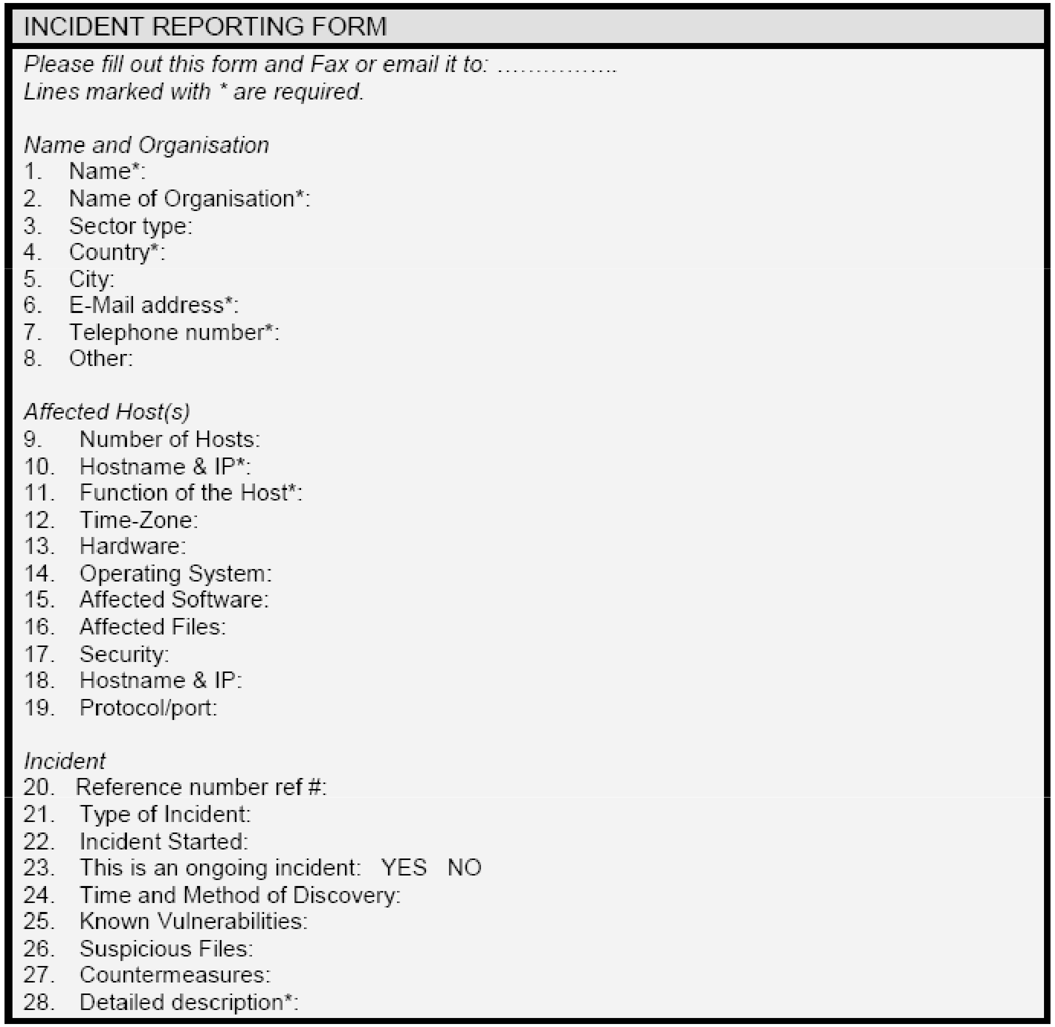
11 Conclusion 61

12 Description of the Project Plan 62

APPENDIX 64

A.1 FURTHER READING 64
A.2 CSIRT SERVICES 65
A.3 THE EXAMPLES 74
A.4 SAMPLE MATERIAL FROM CSIRT COURSES 78

CSIRT: Incident Reporting Form



INCIDENT REPORTING FORM

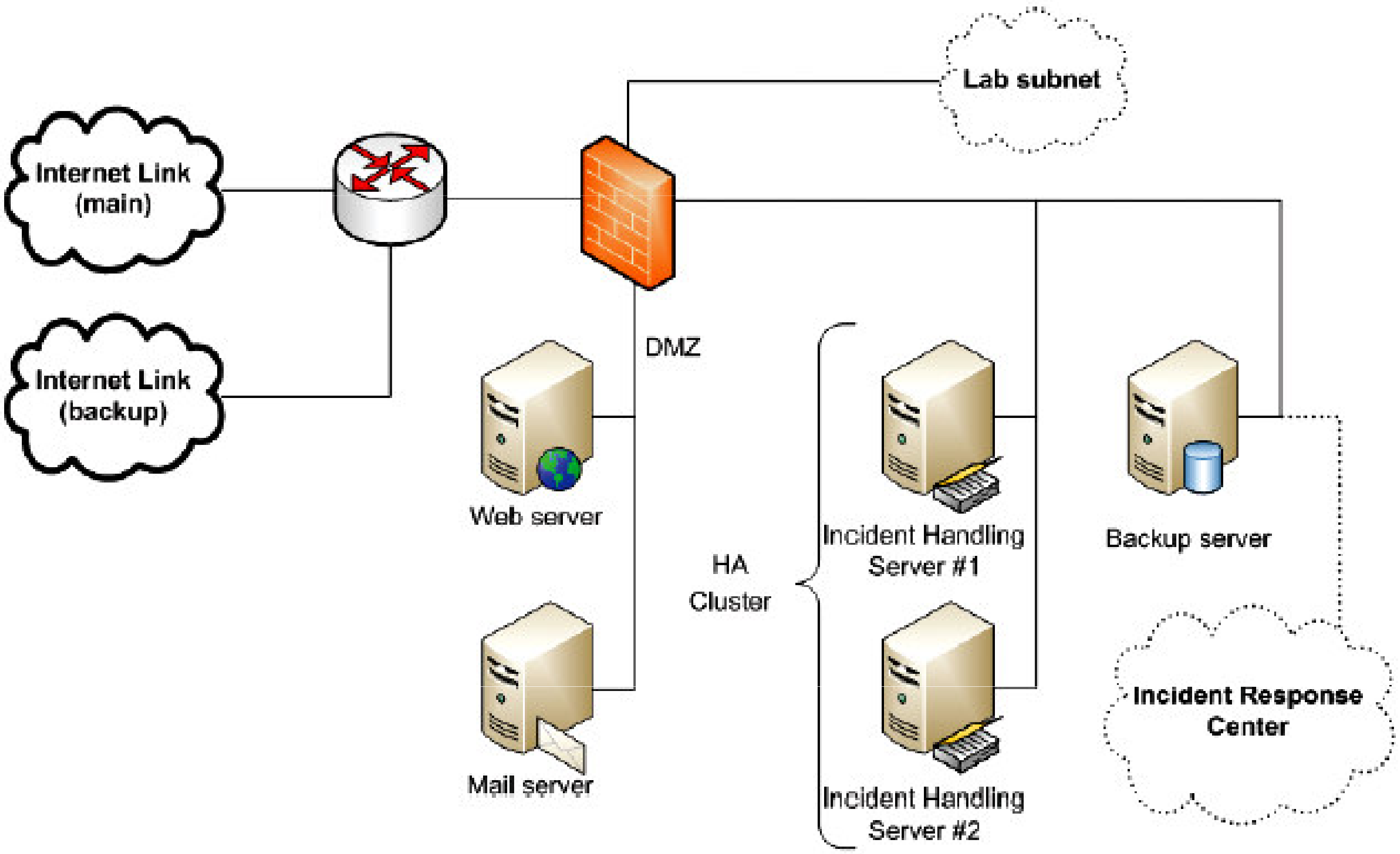
Please fill out this form and Fax or email it to: …………….
*Lines marked with * are required.*

Name and Organisation
1. Name*:
2. Name of Organisation*:
3. Sector type:
4. Country*:
5. City:
6. E-Mail address*:
7. Telephone number*:
8. Other:

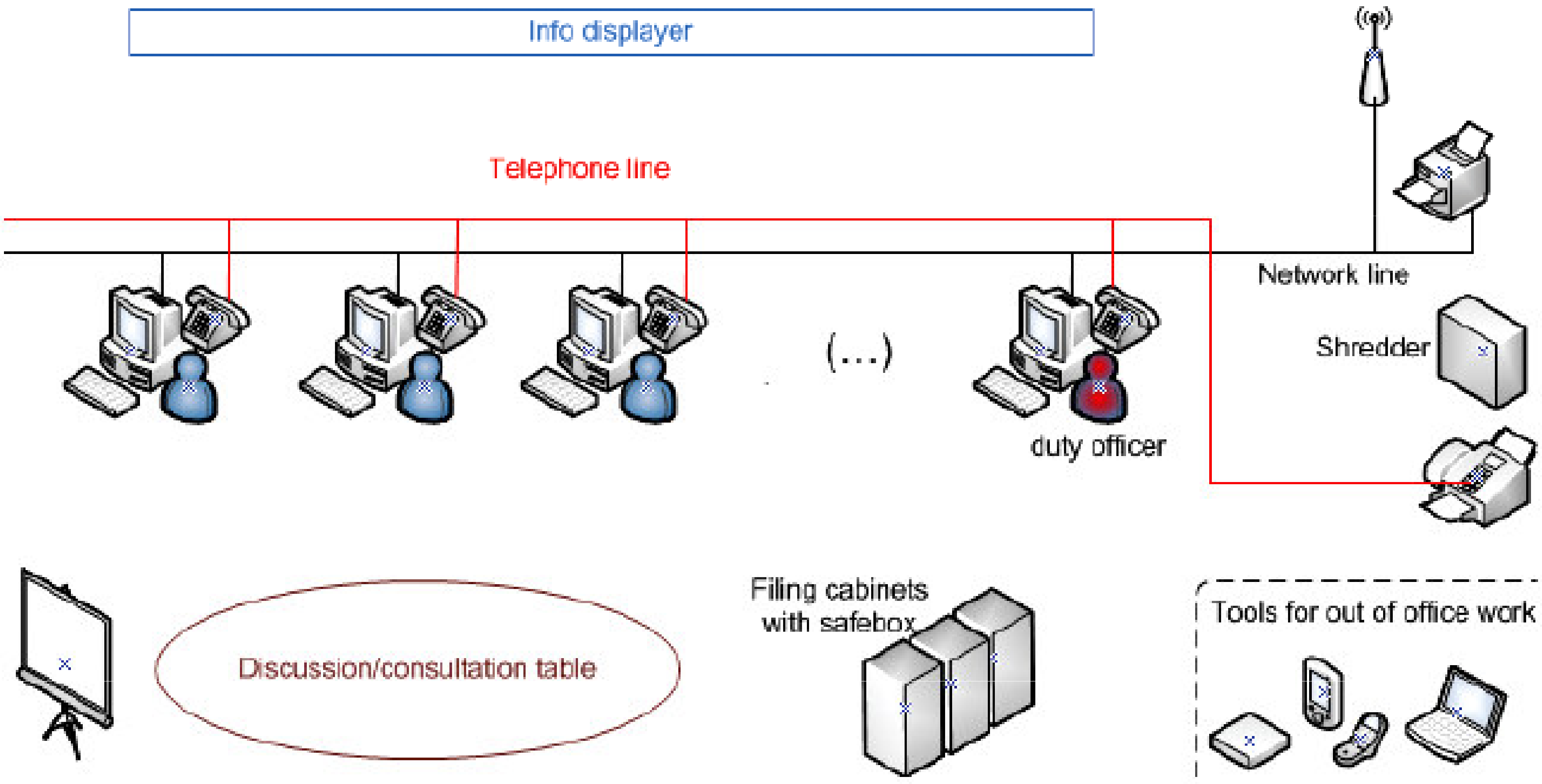
Affected Host(s)
9. Number of Hosts:
10. Hostname & IP*:
11. Function of the Host*:
12. Time-Zone:
13. Hardware:
14. Operating System:
15. Affected Software:
16. Affected Files:
17. Security:
18. Hostname & IP:
19. Protocol/port:

Incident
20. Reference number ref #:
21. Type of Incident:
22. Incident Started:
23. This is an ongoing incident: YES NO
24. Time and Method of Discovery:
25. Known Vulnerabilities:
26. Suspicious Files:
27. Countermeasures:
28. Detailed description*:

Typical CERT Network Infrastructure



CERT Incident Response Centre



ENISA: CERT Exercises and Pilots

ENISA CERT Exercises pilots

November 2009

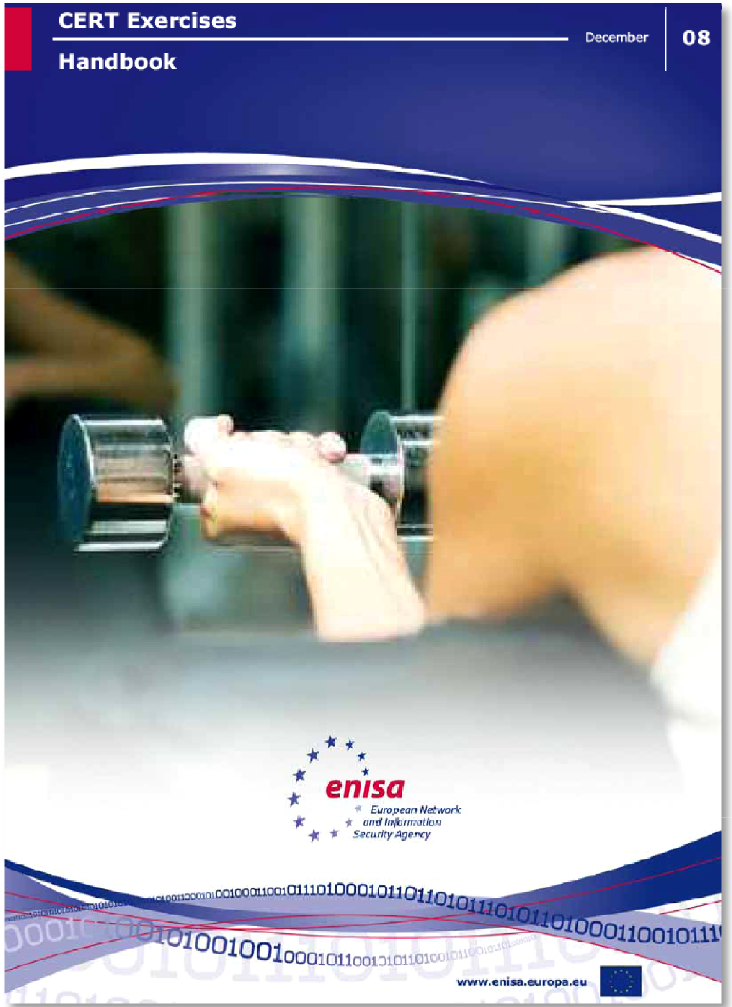
Field Report

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

December 08

Handbook

enisa
European Network and Information Security Agency

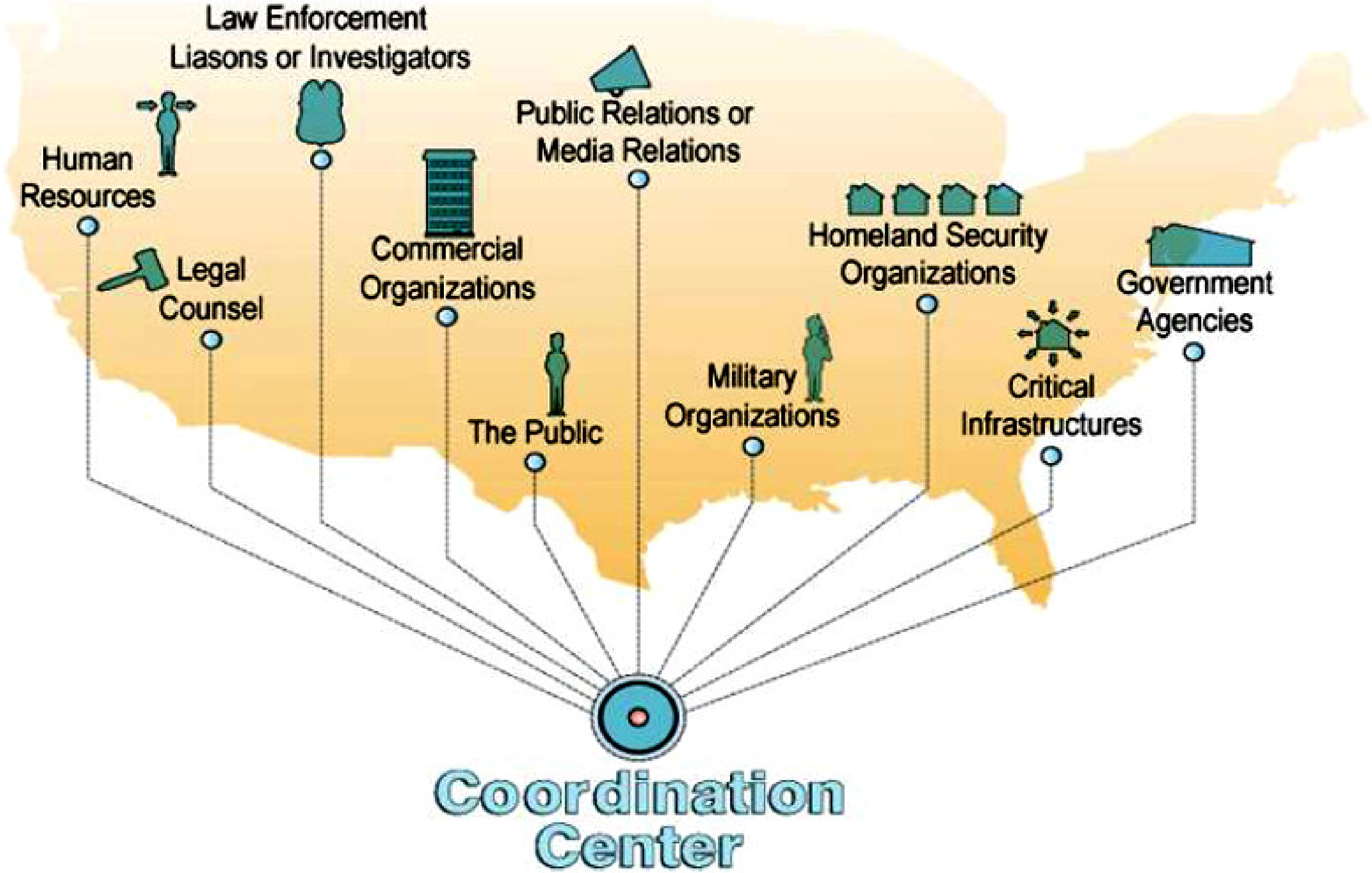
www.enisa.europa.eu

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

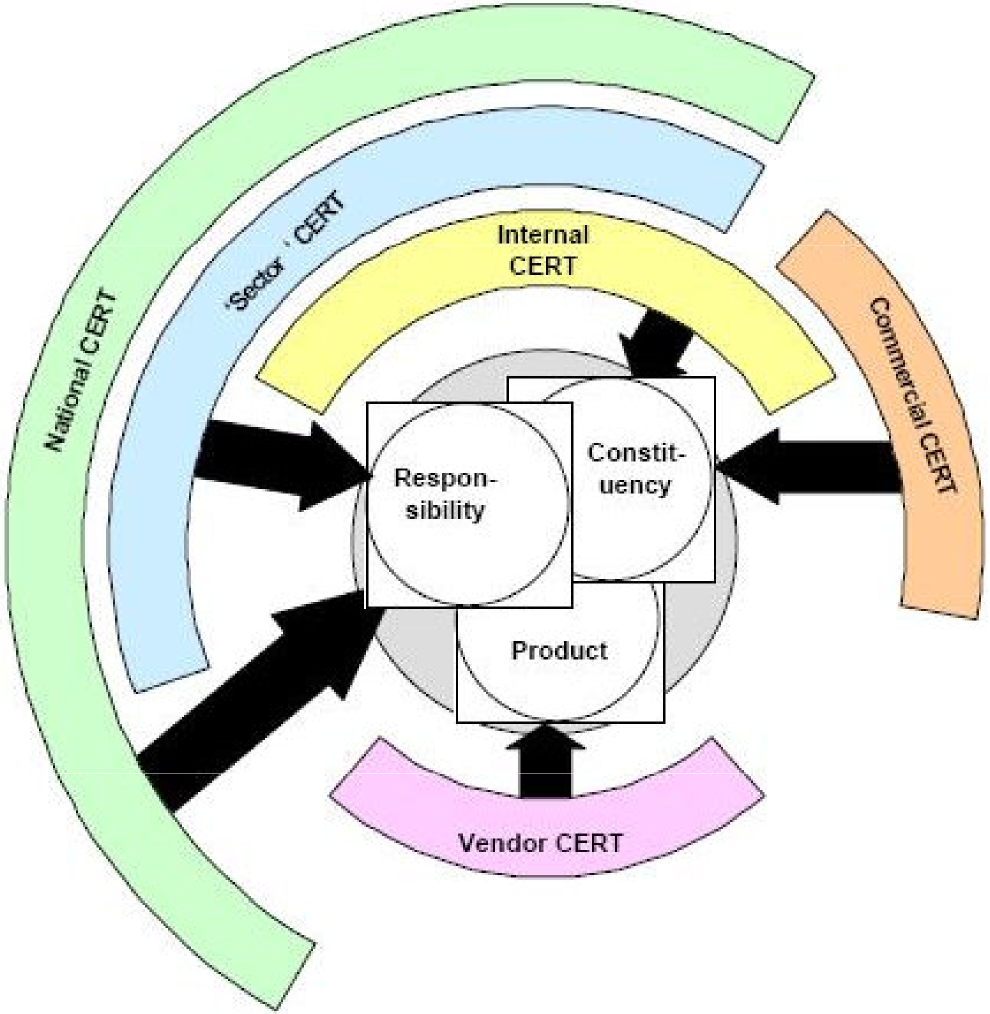
ENISA: CERT Training Video

5min Video Highlights ENISA CERT Training Exercises & Pilots in Japan & Moldova

Working with Stakeholders to create National CERT/CSIRT



Networks of Public & Private CERTs



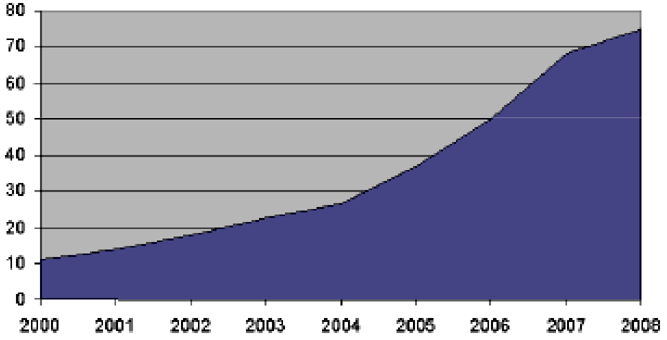
* Workshop Session 6 *

Organising a National Cybercrime Unit (NCU) and National CERT/CSIRT

1–Special Cyber Organisations	2 – CERT/CSIRT Organisation	3 – CERT/CSIRT Alert Centre
4 – CERT/CSIRT: Roll-Out Plan	5 – National Cybercrime Unit	6 – National Cybercrime Unit
7 – ITU: IMPACT Programme	8 – ITU: IMPACT Programme	9 –“Best Practice” for Jamaica

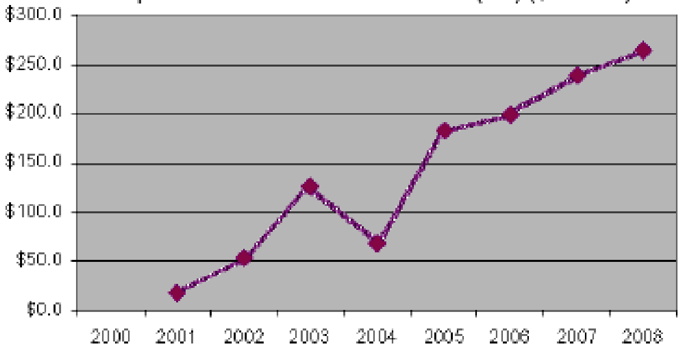
Annual Growth in Cybercrime

Active domains worldwide (millions)



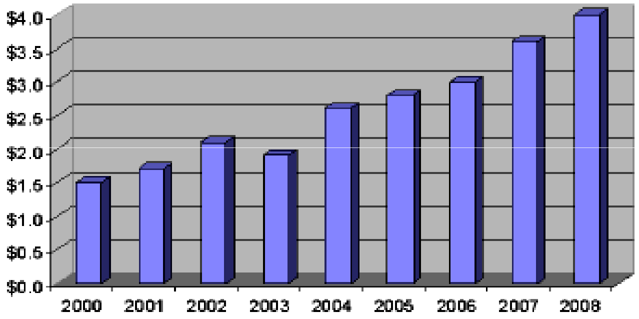
Source: Netcraft Ltd Web Server Survey, April 2009 [5]

Reported losses from Internet crime (US) ($millions)



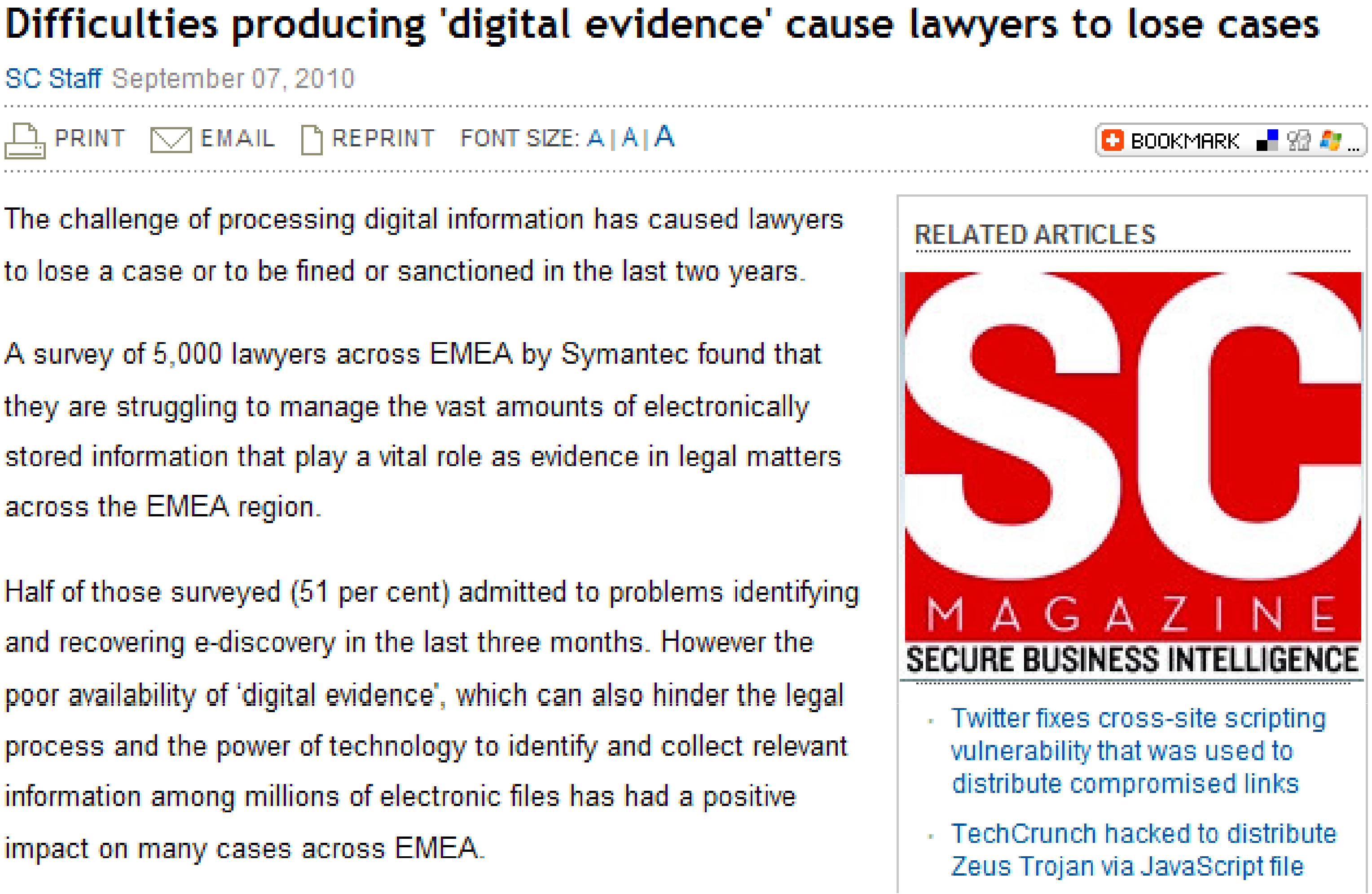
Source: Internet Crime Complaints Center (IC3) Internet Crime Report 2008 [8]

Online revenue loss due to fraud (US & Can) ($billions)



Source: CyberSource Online Fraud Report 2009 [7]

Digital Evidence for e-Crimes



Difficulties producing 'digital evidence' cause lawyers to lose cases

SC Staff September 07, 2010

The challenge of processing digital information has caused lawyers to lose a case or to be fined or sanctioned in the last two years.

A survey of 5,000 lawyers across EMEA by Symantec found that they are struggling to manage the vast amounts of electronically stored information that play a vital role as evidence in legal matters across the EMEA region.

Half of those surveyed (51 per cent) admitted to problems identifying and recovering e-discovery in the last three months. However the poor availability of 'digital evidence', which can also hinder the legal process and the power of technology to identify and collect relevant information among millions of electronic files has had a positive impact on many cases across EMEA.

RELATED ARTICLES

- Twitter fixes cross-site scripting vulnerability that was used to distribute compromised links
- TechCrunch hacked to distribute Zeus Trojan via JavaScript file

National Cybercrime Unit – *"Skills"*

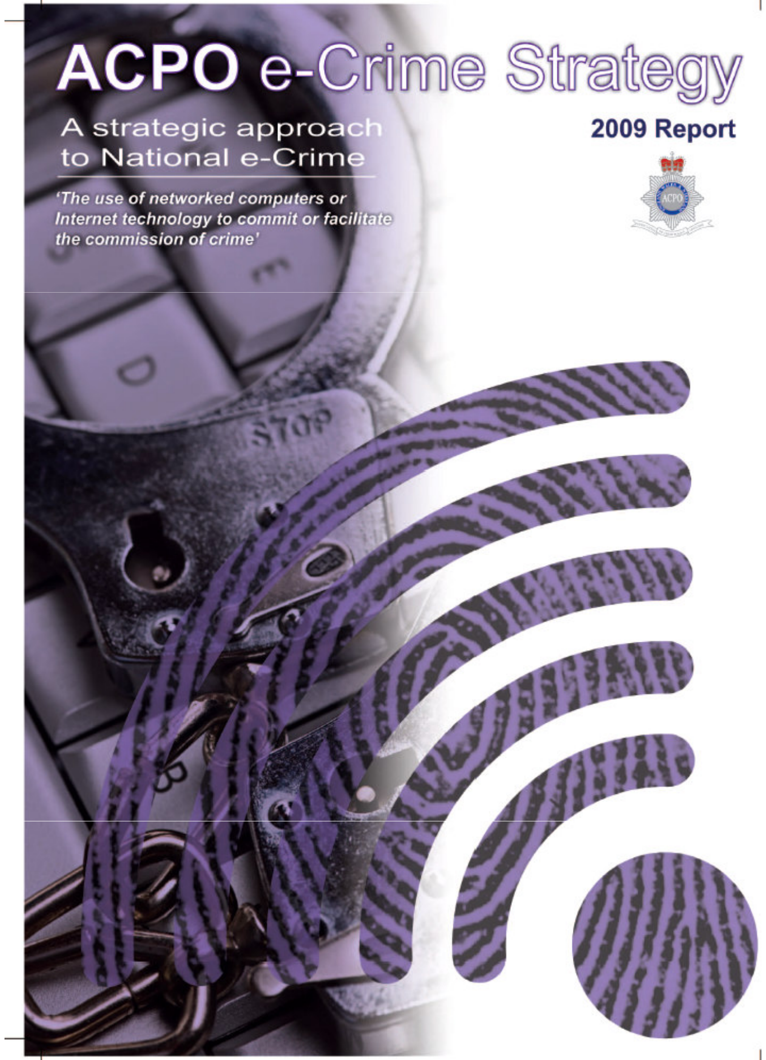
- Jamaica already has an established eCrime Unit so this workshop section will provide some guidelines based upon the UK experience

Jamaica : JCF–OCID –*"Jamaican Constabulary Force –Organised Crime Investigative Division"*

- The UK PCeU – Police Central eCrime Unit has published several excellent documents that will be useful to the Jamaican JCF:
  - National eCrime Strategy
  - National eCrime Programme Structure
  - Good Practice Guide for Computer-Based Evidence
  - eCrime Manager's Guide
  - Download Link: www.met.police.uk/pceu/

- eCrime Unit require some rather specific skills including:
  - *Digital Forensics*: Analysis of information & data on a diverse range of devices, gadgets that may have been used by cybercriminals, sometimes in encrypted formats
  - *Evidence Collection and Classification:* Electronic evidence on devices such as PDAs, and Smart Mobiles may be transitory, and easy lost, deleted or corrupted either locally or by remote radio command. Hence the investigation of cybercrimes requires specialist training

Strategic Approach to National e-Crime

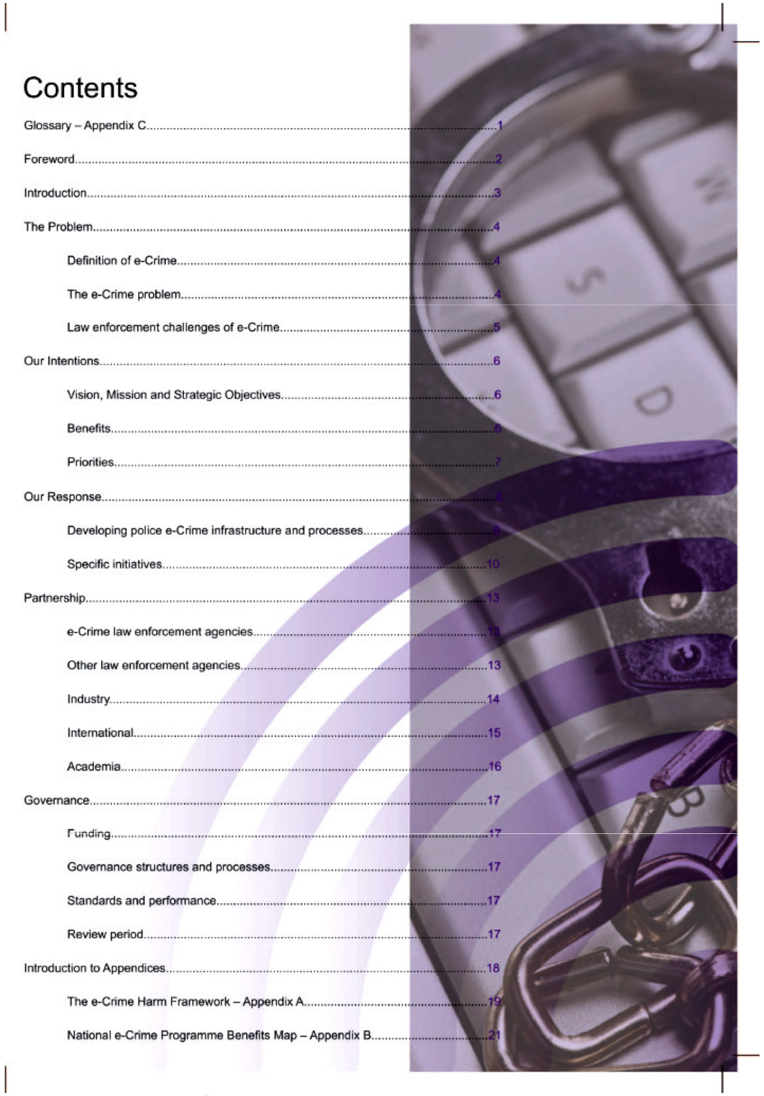


ACPO e-Crime Strategy

A strategic approach to National e-Crime

2009 Report

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



Contents

Glossary – Appendix C........1

Foreword........2

Introduction........3

The Problem........4

Definition of e-Crime........4

The e-Crime problem........4

Law enforcement challenges of e-Crime........5

Our Intentions........6

Vision, Mission and Strategic Objectives........6

Benefits........6

Priorities........7

Our Response........8

Developing police e-Crime infrastructure and processes........8

Specific initiatives........10

Partnership........13

e-Crime law enforcement agencies........13

Other law enforcement agencies........13

Industry........14

International........15

Academia........16

Governance........17

Funding........17

Governance structures and processes........17

Standards and performance........17

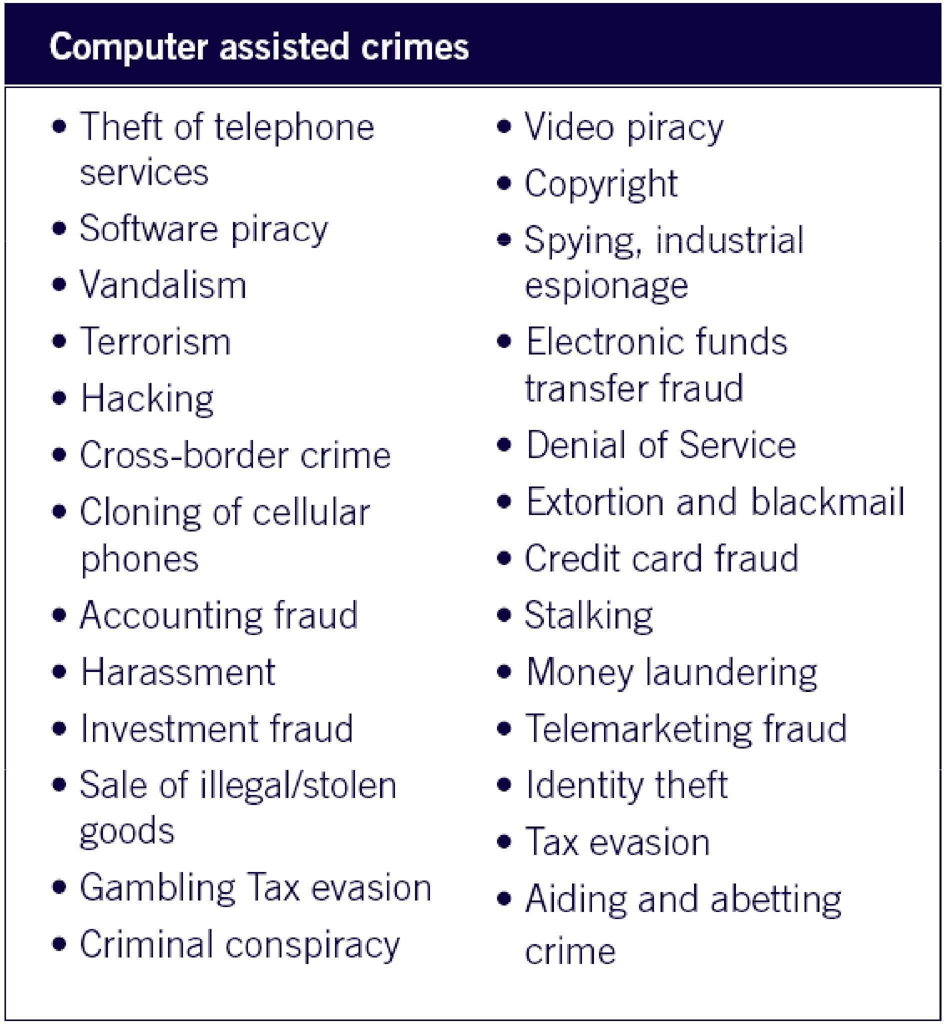
Review period........17

Introduction to Appendices........18

The e-Crime Harm Framework – Appendix A........19

National e-Crime Programme Benefits Map – Appendix B........21

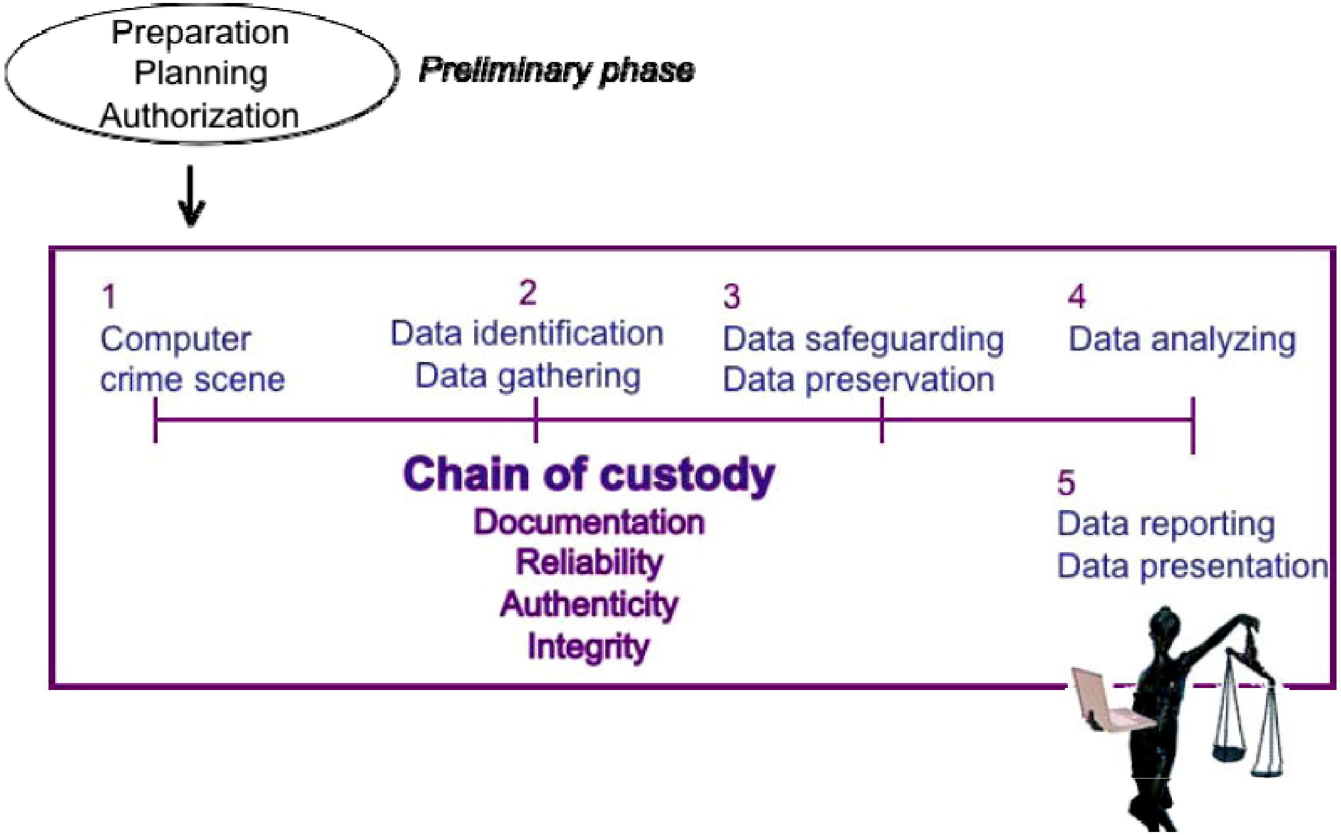
Scale and Nature of e-Crimes



Computer assisted crimes

- Theft of telephone services
- Software piracy
- Vandalism
- Terrorism
- Hacking
- Cross-border crime
- Cloning of cellular phones
- Accounting fraud
- Harassment
- Investment fraud
- Sale of illegal/stolen goods
- Gambling Tax evasion
- Criminal conspiracy
- Video piracy
- Copyright
- Spying, industrial espionage
- Electronic funds transfer fraud
- Denial of Service
- Extortion and blackmail
- Credit card fraud
- Stalking
- Money laundering
- Telemarketing fraud
- Identity theft
- Tax evasion
- Aiding and abetting crime

Cybercrime Investigation Methodology



Preparation
Planning
Authorization

Preliminary phase

1
Computer
crime scene

2
Data identification
Data gathering

3
Data safeguarding
Data preservation

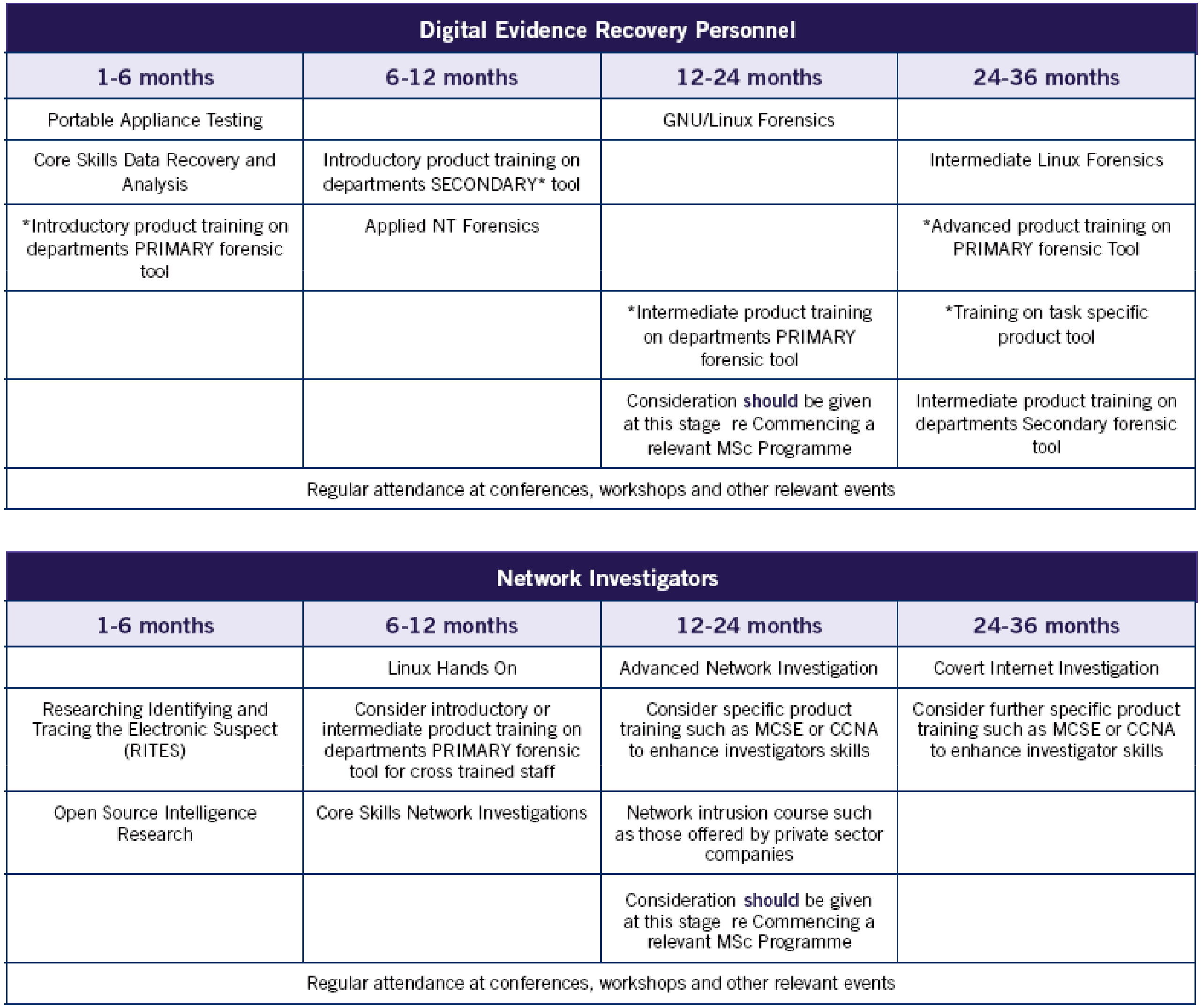
4
Data analyzing

Chain of custody
Documentation
Reliability
Authenticity
Integrity

5
Data reporting
Data presentation

Figure III.2: Computer crime investigation methodology

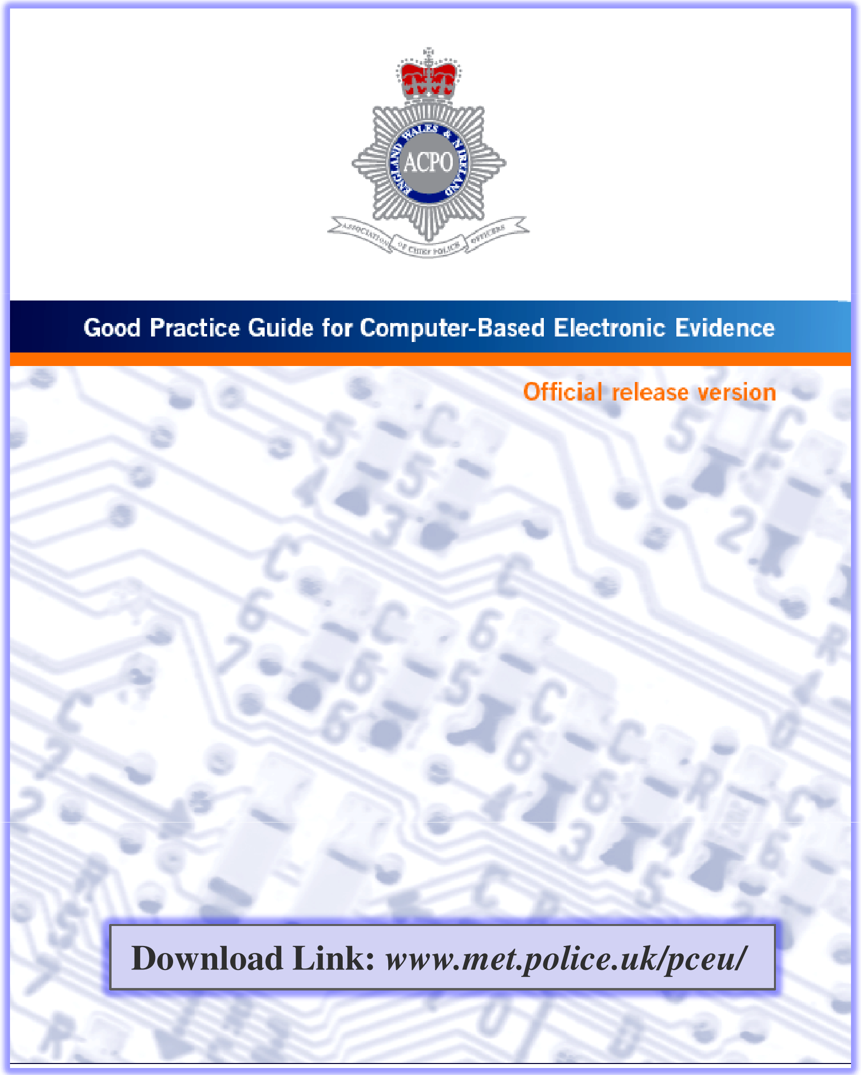
E-Crime Personnel Training Matrix



Digital Evidence Recovery Personnel			
1-6 months	**6-12 months**	**12-24 months**	**24-36 months**
Portable Appliance Testing		GNU/Linux Forensics	
Core Skills Data Recovery and Analysis	Introductory product training on departments SECONDARY* tool		Intermediate Linux Forensics
*Introductory product training on departments PRIMARY forensic tool	Applied NT Forensics		*Advanced product training on PRIMARY forensic Tool
		*Intermediate product training on departments PRIMARY forensic tool	*Training on task specific product tool
		Consideration **should** be given at this stage re Commencing a relevant MSc Programme	Intermediate product training on departments Secondary forensic tool
Regular attendance at conferences, workshops and other relevant events			

Network Investigators			
1-6 months	**6-12 months**	**12-24 months**	**24-36 months**
	Linux Hands On	Advanced Network Investigation	Covert Internet Investigation
Researching Identifying and Tracing the Electronic Suspect (RITES)	Consider introductory or intermediate product training on departments PRIMARY forensic tool for cross trained staff	Consider specific product training such as MCSE or CCNA to enhance investigators skills	Consider further specific product training such as MCSE or CCNA to enhance investigator skills
Open Source Intelligence Research	Core Skills Network Investigations	Network intrusion course such as those offered by private sector companies	
		Consideration **should** be given at this stage re Commencing a relevant MSc Programme	
Regular attendance at conferences, workshops and other relevant events			

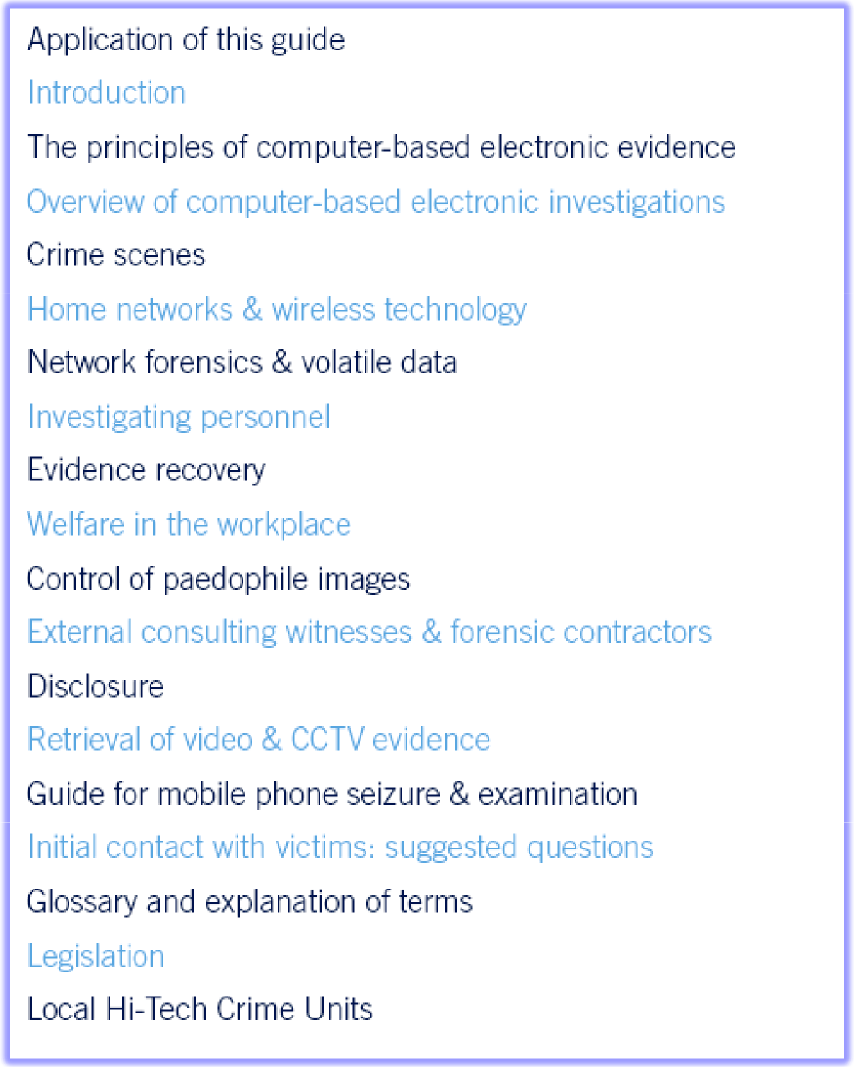
UK Guide to Computer-Based Electronic Evidence



Good Practice Guide for Computer-Based Electronic Evidence

Official release version

Download Link: ***www.met.police.uk/pceu/***



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

* Workshop Session 6 *

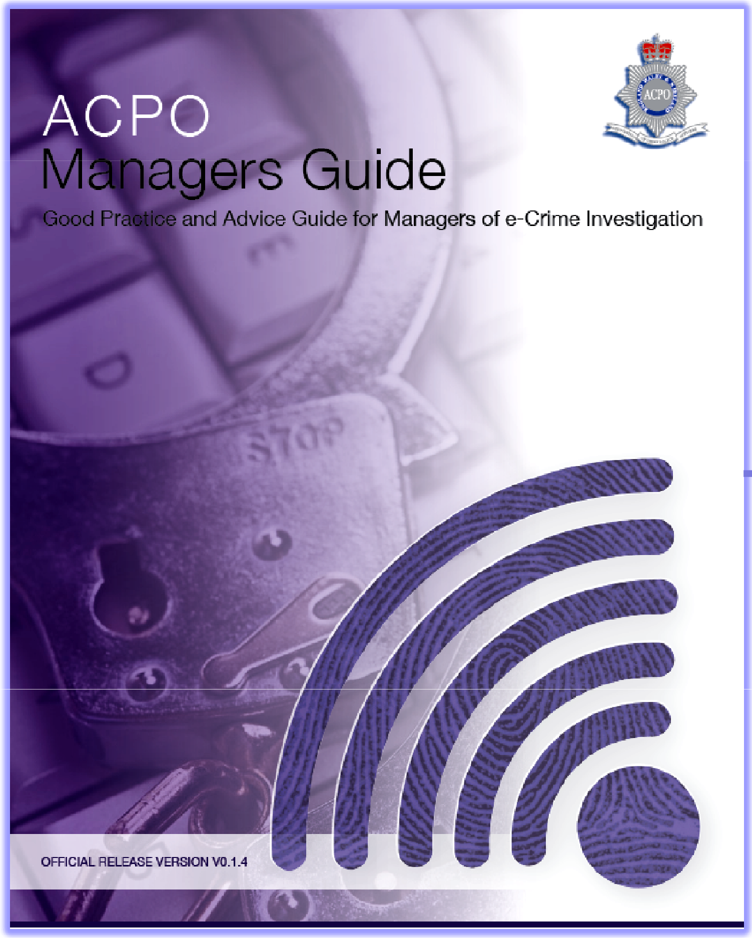
Organising a National Cybercrime Unit (NCU) and National CERT/CSIRT

1–Special Cyber Organisations	2 – CERT/CSIRT Organisation	3 – CERT/CSIRT Alert Centre
4 – CERT/CSIRT: Roll-Out Plan	5 – National Cybercrime Unit	6 – National Cybercrime Unit
7 – ITU: IMPACT Programme	8 – ITU: IMPACT Programme	9 –"Best Practice" for Jamaica

National Cybercrime Unit – "*Admin*"

- Most National eCrime Units are less than 5 years old and are still developing their skills, capabilities & reputations. "*Learning is real-time!*"
- Establishing and Managing and eCrime Unit requires consultation with a range of stakeholders both inside and outside the civil police forces.
- eCrime Units can only effectively tackle crime if the Government has already put in place relevant cybercrime legislation spanning the spectrum of cybercrimes and attacks that we've already discussed in the workshop
- Key priorities will be the integration within the traditional Civil Police Force, and the wider communication of the eCrime Unit's Role and Responsibilities both within the Police Force and also Business & Citizens
- ….In the next few slides we'll explore some of the top management topics & themes from the UK Manager's Guide to eCrime Investigations

Manager's Guide to e-Crime Investigations: UK e-Crime Unit



ACPO
Managers Guide
Good Practice and Advice Guide for Managers of e-Crime Investigation

OFFICIAL RELEASE VERSION V0.1.4

Contents

Introduction

Initial Set-up

Management Matters

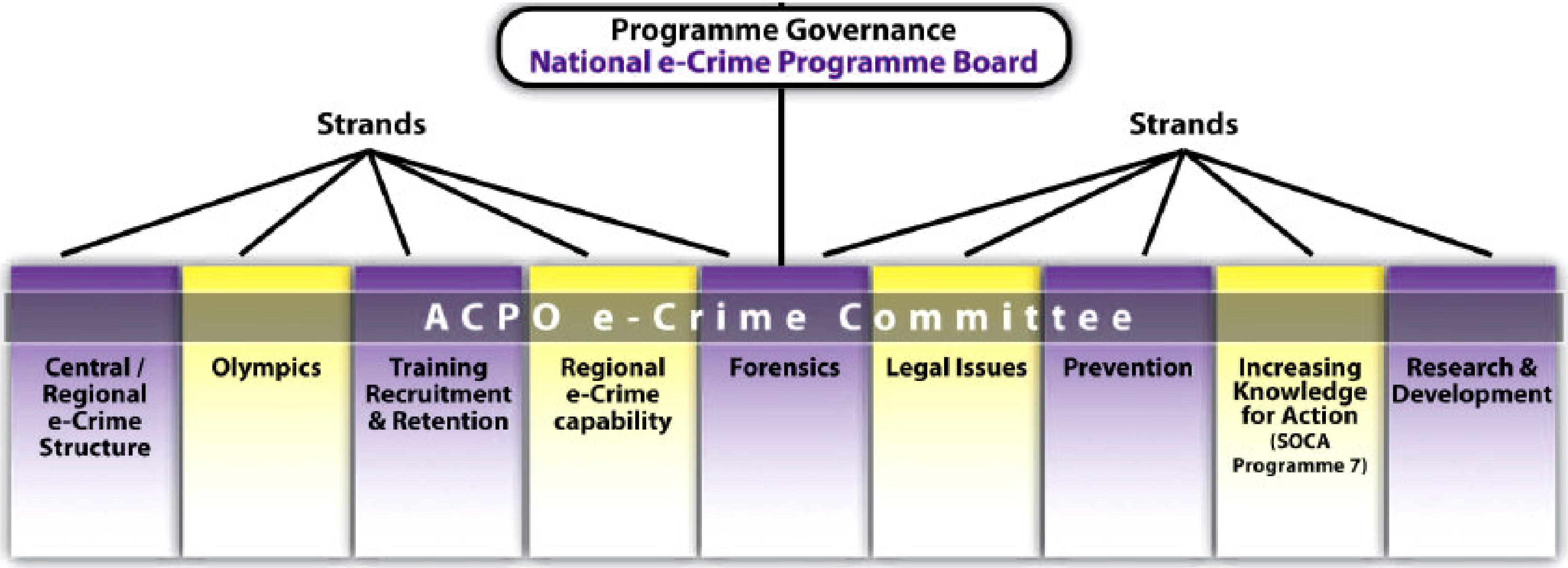
Investigation Matters

General Issues

Forensic Issues

Training

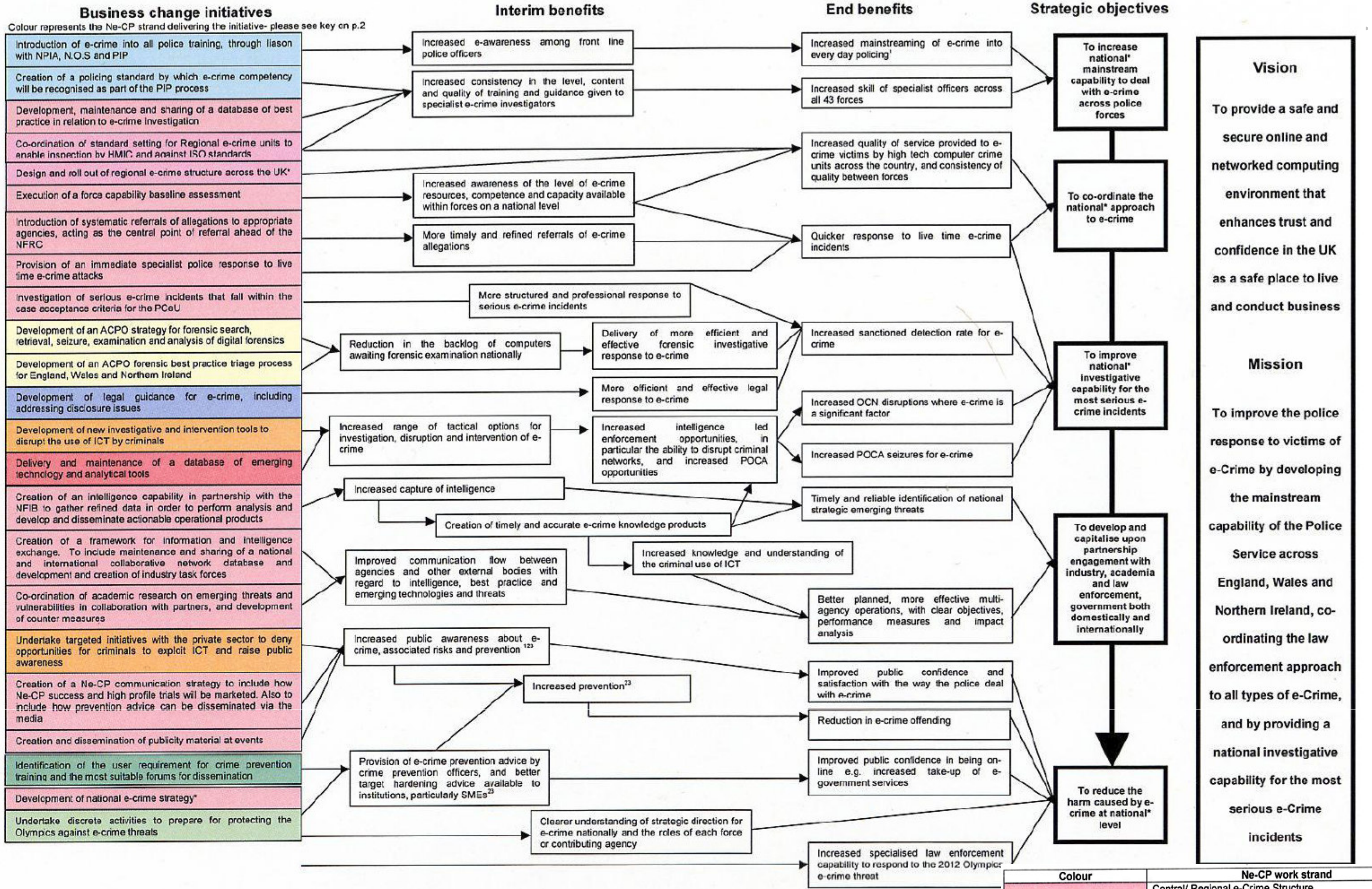
Organisation of the UK e-Crime Programme Board



Programme Governance
National e-Crime Programme Board
Strands
Strands
ACPO e-Crime Committee
Central / Regional e-Crime Structure
Olympics
Training Recruitment & Retention
Regional e-Crime capability
Forensics
Legal Issues
Prevention
Increasing Knowledge for Action (SOCA Programme 7)
Research & Development

Jamaica : JCF – OCID – *"Jamaican Constabulary Force – Organised Crime Investigative Division"*

National e-Crime Programme Benefits Map



Business change initiatives

Colour represents the Ne-CP strand delivering the initiative- please see key on p.2

- Introduction of e-crime into all police training, through liason with NPIA, N.O.S and PIP
- Creation of a policing standard by which e-crime competency will be recognised as part of the PIP process
- Development, maintenance and sharing of a database of best practice in relation to e-crime investigation
- Co-ordination of standard setting for Regional e-crime units to enable inspection by HMIC and against ISO standards
- Design and roll out of regional e-crime structure across the UK*
- Execution of a force capability baseline assessment
- Introduction of systematic referrals of allegations to appropriate agencies, acting as the central point of referral ahead of the NFRC
- Provision of an immediate specialist police response to live time e-crime attacks
- Investigation of serious e-crime incidents that fall within the case acceptance criteria for the PCeU
- Development of an ACPO strategy for forensic search, retrieval, seizure, examination and analysis of digital forensics
- Development of an ACPO forensic best practice triage process for England, Wales and Northern Ireland
- Development of legal guidance for e-crime, including addressing disclosure issues
- Development of new investigative and intervention tools to disrupt the use of ICT by criminals
- Delivery and maintenance of a database of emerging technology and analytical tools
- Creation of an intelligence capability in partnership with the NFIB to gather refined data in order to perform analysis and develop and disseminate actionable operational products
- Creation of a framework for information and intelligence exchange. To include maintenance and sharing of a national and international collaborative network database and development and creation of industry task forces
- Co-ordination of academic research on emerging threats and vulnerabilities in collaboration with partners, and development of counter measures
- Undertake targeted initiatives with the private sector to deny opportunities for criminals to exploit ICT and raise public awareness
- Creation of a Ne-CP communication strategy to include how Ne-CP success and high profile trials will be marketed. Also to include how prevention advice can be disseminated via the media
- Creation and dissemination of publicity material at events
- Identification of the user requirement for crime prevention training and the most suitable forums for dissemination
- Development of national e-crime strategy*
- Undertake discrete activities to prepare for protecting the Olympics against e-crime threats

Interim benefits

- Increased e-awareness among front line police officers
- Increased consistency in the level, content and quality of training and guidance given to specialist e-crime investigators
- Increased awareness of the level of e-crime resources, competence and capacity available within forces on a national level
- More timely and refined referrals of e-crime allegations
- More structured and professional response to serious e-crime incidents
- Reduction in the backlog of computers awaiting forensic examination nationally
- Delivery of more efficient and effective forensic investigative response to e-crime
- More efficient and effective legal response to e-crime
- Increased range of tactical options for investigation, disruption and intervention of e-crime
- Increased intelligence led enforcement opportunities, in particular the ability to disrupt criminal networks, and increased POCA opportunities
- Increased capture of intelligence
- Creation of timely and accurate e-crime knowledge products
- Increased knowledge and understanding of the criminal use of ICT
- Improved communication flow between agencies and other external bodies with regard to intelligence, best practice and emerging technologies and threats
- Increased public awareness about e-crime, associated risks and prevention [123]
- Increased prevention[23]
- Provision of e-crime prevention advice by crime prevention officers, and better target hardening advice available to institutions, particularly SMEs[23]
- Clearer understanding of strategic direction for e-crime nationally and the roles of each force or contributing agency

End benefits

- Increased mainstreaming of e-crime into every day policing[1]
- Increased skill of specialist officers across all 43 forces
- Increased quality of service provided to e-crime victims by high tech computer crime units across the country, and consistency of quality between forces
- Quicker response to live time e-crime incidents
- Increased sanctioned detection rate for e-crime
- Increased OCN disruptions where e-crime is a significant factor
- Increased POCA seizures for e-crime
- Timely and reliable identification of national strategic emerging threats
- Better planned, more effective multi-agency operations, with clear objectives, performance measures and impact analysis
- Improved public confidence and satisfaction with the way the police deal with e-crime
- Reduction in e-crime offending
- Improved public confidence in being on-line e.g. increased take-up of e-government services
- Increased specialised law enforcement capability to respond to the 2012 Olympics e-crime threat

Strategic objectives

- To increase national* mainstream capability to deal with e-crime across police forces
- To co-ordinate the national* approach to e-crime
- To improve national* investigative capability for the most serious e-crime incidents
- To develop and capitalise upon partnership engagement with industry, academia and law enforcement, government both domestically and internationally
- To reduce the harm caused by e-crime at national* level

Vision

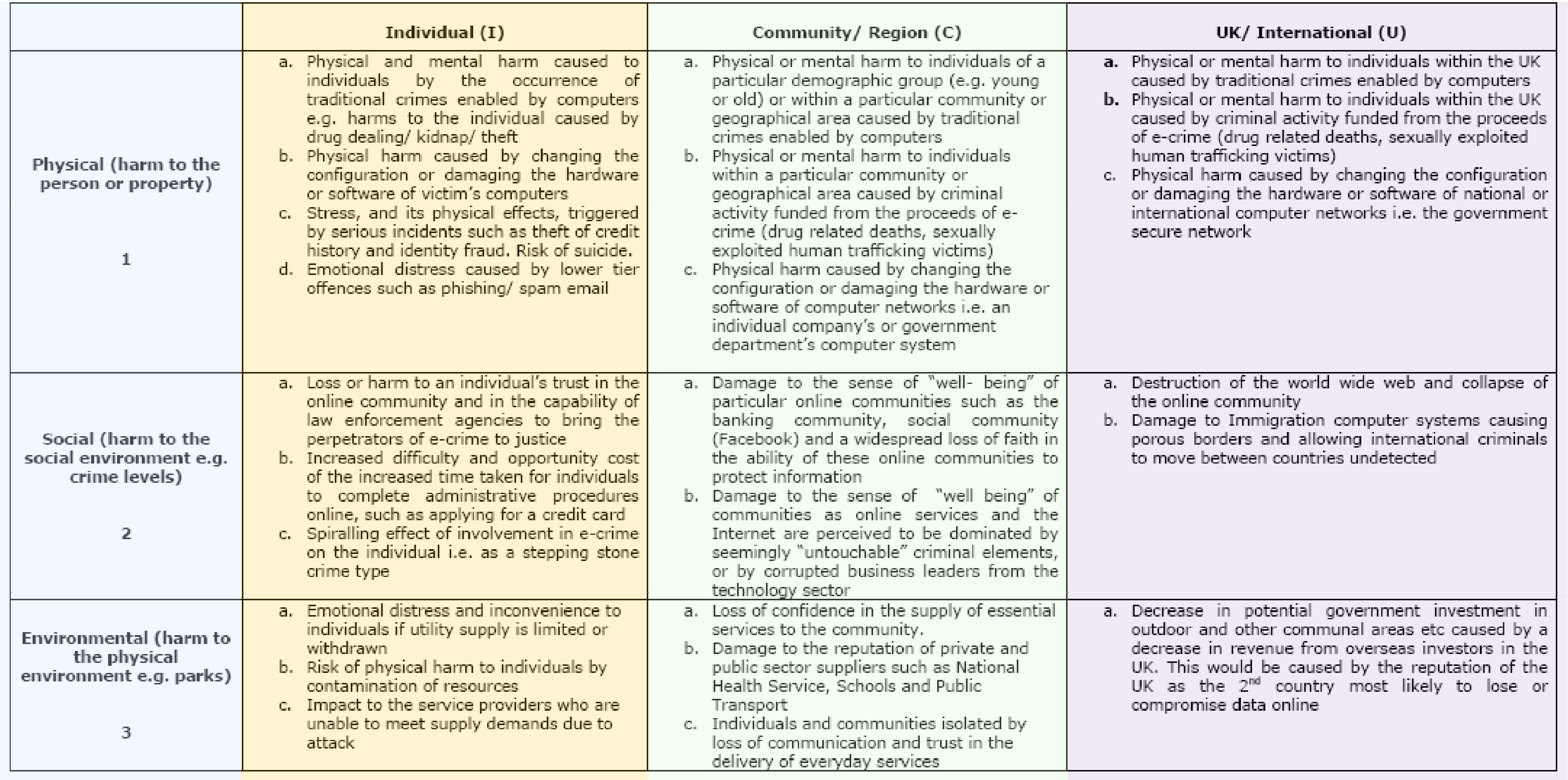
To provide a safe and secure online and networked computing environment that enhances trust and confidence in the UK as a safe place to live and conduct business

Mission

To improve the police response to victims of e-Crime by developing the mainstream capability of the Police Service across England, Wales and Northern Ireland, co-ordinating the law enforcement approach to all types of e-Crime, and by providing a national investigative capability for the most serious e-Crime incidents

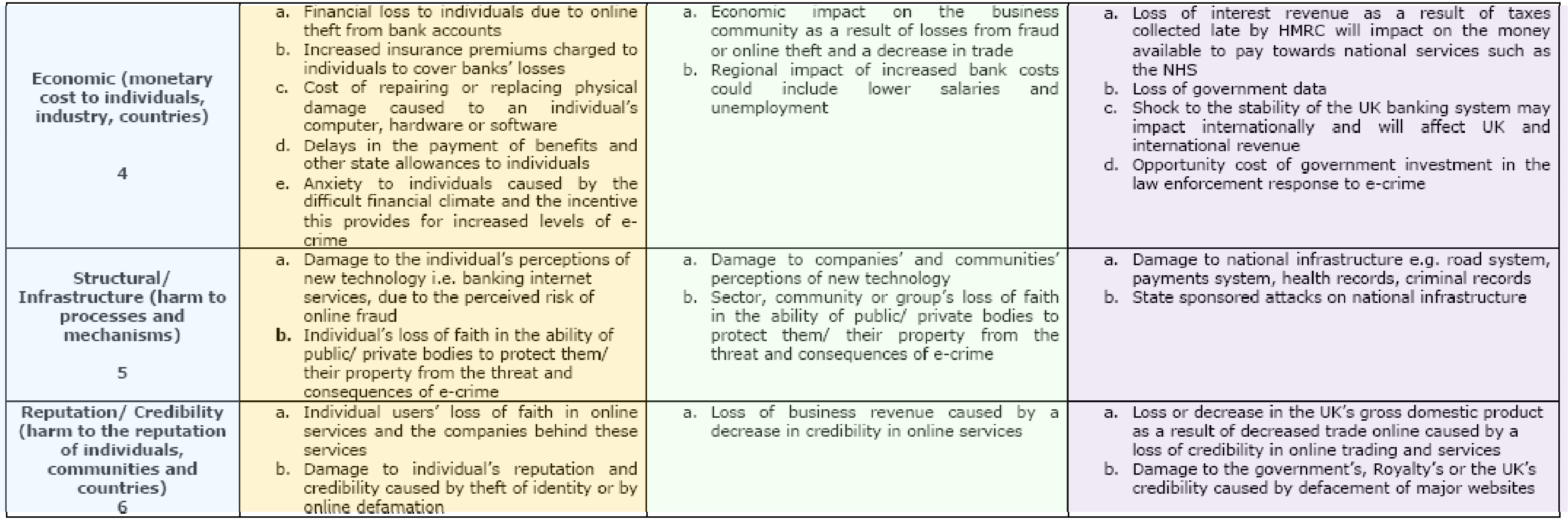
Colour	Ne-CP work strand
🟪	Central/ Regional e-Crime Structure
🟦	Training, recruitment and retention
🟪	Regional e-Crime Units
🟨	Forensics
🟦	Legal Issues
🟩	Prevention
🟧	Increasing Knowledge for Action (SOCA Programme 7)
🟥	Research and Development
🟩	Olympics

"Harm" Impact Framework: UK e-Crime (1)



	Individual (I)	Community/ Region (C)	UK/ International (U)
Physical (harm to the person or property) 1	a. Physical and mental harm caused to individuals by the occurrence of traditional crimes enabled by computers e.g. harms to the individual caused by drug dealing/ kidnap/ theft b. Physical harm caused by changing the configuration or damaging the hardware or software of victim's computers c. Stress, and its physical effects, triggered by serious incidents such as theft of credit history and identity fraud. Risk of suicide. d. Emotional distress caused by lower tier offences such as phishing/ spam email	a. Physical or mental harm to individuals of a particular demographic group (e.g. young or old) or within a particular community or geographical area caused by traditional crimes enabled by computers b. Physical or mental harm to individuals within a particular community or geographical area caused by criminal activity funded from the proceeds of e-crime (drug related deaths, sexually exploited human trafficking victims) c. Physical harm caused by changing the configuration or damaging the hardware or software of computer networks i.e. an individual company's or government department's computer system	**a.** Physical or mental harm to individuals within the UK caused by traditional crimes enabled by computers **b.** Physical or mental harm to individuals within the UK caused by criminal activity funded from the proceeds of e-crime (drug related deaths, sexually exploited human trafficking victims) c. Physical harm caused by changing the configuration or damaging the hardware or software of national or international computer networks i.e. the government secure network
Social (harm to the social environment e.g. crime levels) 2	a. Loss or harm to an individual's trust in the online community and in the capability of law enforcement agencies to bring the perpetrators of e-crime to justice b. Increased difficulty and opportunity cost of the increased time taken for individuals to complete administrative procedures online, such as applying for a credit card c. Spiralling effect of involvement in e-crime on the individual i.e. as a stepping stone crime type	a. Damage to the sense of "well- being" of particular online communities such as the banking community, social community (Facebook) and a widespread loss of faith in the ability of these online communities to protect information b. Damage to the sense of "well being" of communities as online services and the Internet are perceived to be dominated by seemingly "untouchable" criminal elements, or by corrupted business leaders from the technology sector	a. Destruction of the world wide web and collapse of the online community b. Damage to Immigration computer systems causing porous borders and allowing international criminals to move between countries undetected
Environmental (harm to the physical environment e.g. parks) 3	a. Emotional distress and inconvenience to individuals if utility supply is limited or withdrawn b. Risk of physical harm to individuals by contamination of resources c. Impact to the service providers who are unable to meet supply demands due to attack	a. Loss of confidence in the supply of essential services to the community. b. Damage to the reputation of private and public sector suppliers such as National Health Service, Schools and Public Transport c. Individuals and communities isolated by loss of communication and trust in the delivery of everyday services	a. Decrease in potential government investment in outdoor and other communal areas etc caused by a decrease in revenue from overseas investors in the UK. This would be caused by the reputation of the UK as the 2nd country most likely to lose or compromise data online

“Harm” Impact Framework: UK e-Crime (2)



Economic (monetary cost to individuals, industry, countries) 4	a. Financial loss to individuals due to online theft from bank accounts b. Increased insurance premiums charged to individuals to cover banks’ losses c. Cost of repairing or replacing physical damage caused to an individual’s computer, hardware or software d. Delays in the payment of benefits and other state allowances to individuals e. Anxiety to individuals caused by the difficult financial climate and the incentive this provides for increased levels of e-crime	a. Economic impact on the business community as a result of losses from fraud or online theft and a decrease in trade b. Regional impact of increased bank costs could include lower salaries and unemployment	a. Loss of interest revenue as a result of taxes collected late by HMRC will impact on the money available to pay towards national services such as the NHS b. Loss of government data c. Shock to the stability of the UK banking system may impact internationally and will affect UK and international revenue d. Opportunity cost of government investment in the law enforcement response to e-crime
Structural/ Infrastructure (harm to processes and mechanisms) 5	a. Damage to the individual’s perceptions of new technology i.e. banking internet services, due to the perceived risk of online fraud b. Individual’s loss of faith in the ability of public/ private bodies to protect them/ their property from the threat and consequences of e-crime	a. Damage to companies’ and communities’ perceptions of new technology b. Sector, community or group’s loss of faith in the ability of public/ private bodies to protect them/ their property from the threat and consequences of e-crime	a. Damage to national infrastructure e.g. road system, payments system, health records, criminal records b. State sponsored attacks on national infrastructure
Reputation/ Credibility (harm to the reputation of individuals, communities and countries) 6	a. Individual users’ loss of faith in online services and the companies behind these services b. Damage to individual’s reputation and credibility caused by theft of identity or by online defamation	a. Loss of business revenue caused by a decrease in credibility in online services	a. Loss or decrease in the UK’s gross domestic product as a result of decreased trade online caused by a loss of credibility in online trading and services b. Damage to the government’s, Royalty’s or the UK’s credibility caused by defacement of major websites

Impacts: (1) ***Physical***; (2) ***Social;*** (3) ***Environmental;*** (4) ***Economic***; (5) ***Structural;*** (6) ***Reputation***;

* Workshop Session 6 *

Organising a National Cybercrime Unit (NCU) and National CERT/CSIRT

1–Special Cyber Organisations	2 – CERT/CSIRT Organisation	3 – CERT/CSIRT Alert Centre
4 – CERT/CSIRT: Roll-Out Plan	5 – National Cybercrime Unit	6 – National Cybercrime Unit
7 – ITU: IMPACT Programme	8 – ITU: IMPACT Programme	9 –"Best Practice" for Jamaica

ITU : IMPACT Programme (A)

- The ITU is one of the key international players in the global alliance with IMPACT with its worldwide headquarters at Cyberjaya, Malaysia

- IMPACT runs 4 major service programmes that are defined as:

  - The Global Response Centre (GRC): Modelled on the CDC in Atlanta, USA, the GRC is designed to be the foremost cyber threats resource centre in the world

  - Centre for Policy and International Co-Operation: IMPACT partnership with the ITU brings a potential memebership of 191 member states. Other International Partners include the United Nations, Interpol, and the Council of Europe (CoE)

  - Centre for Training and Skills Development: IMPACT works on cybersecurity training and certification with many of the world leading companies and organisations.

  - Centre for Security Assurance and Research: In-Depth Research into Data Mining and Threats, Botnets and the development of the IMPACT Research Online Network (IRON). Also the development of the global “CIRT-LITE” Service and the IGSS DashBoard.

…….Next we’ll briefly explore some of the GRC Programmes as well as the Training RoadMap

Features of the Global Resource Centre

- Key Features of the GRC include:

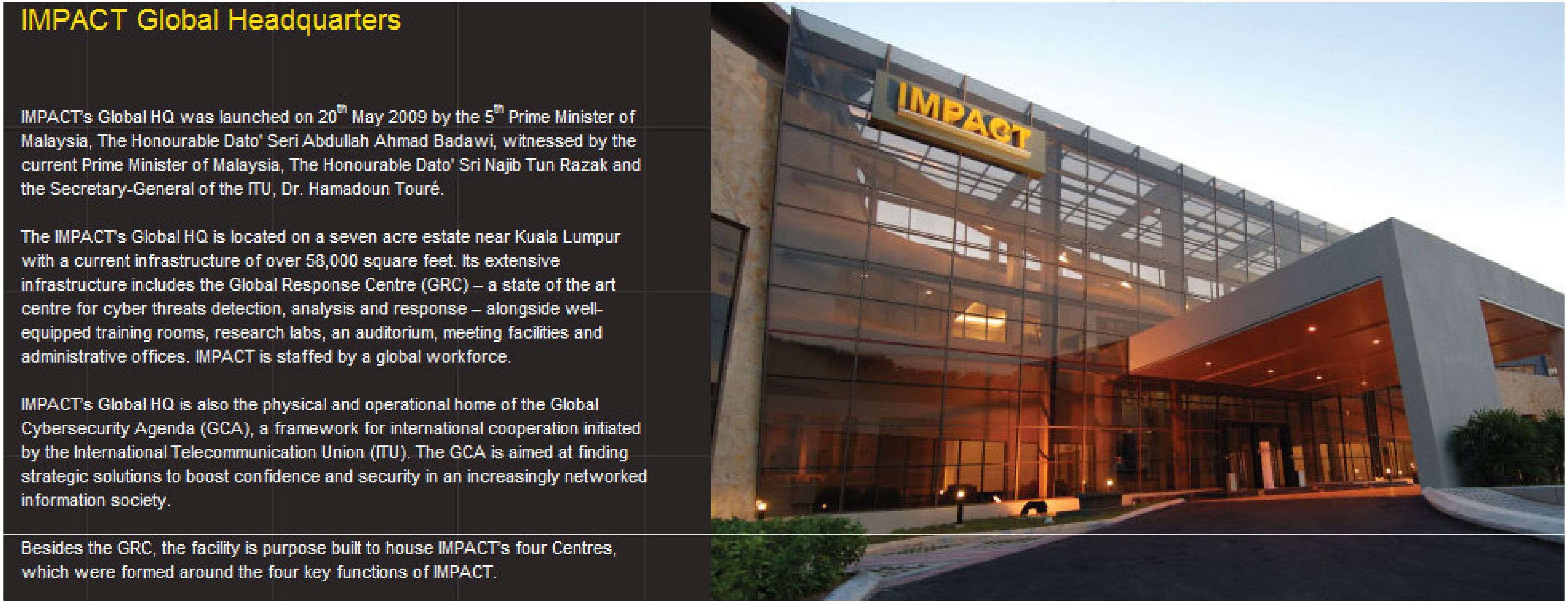
  1) Network Early Warning System
  2) Automated Threat Analysis System (ATAS)
  3) Global Visualisation of Threats
  4) Remediation Facility
  5) Trend Management and Knowledge base
  6) Country Specific Cyber Threat
  7) Incident and Case Management
  8) Trend Monitoring and Analysis
  9) IMPACT Honeypot
  10) Cyber Threat Route Plotter

IMPACT

INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

IMPACT: Global Response Centre

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

Worldwide IMPACT Alliance: Organisation

IMPACT

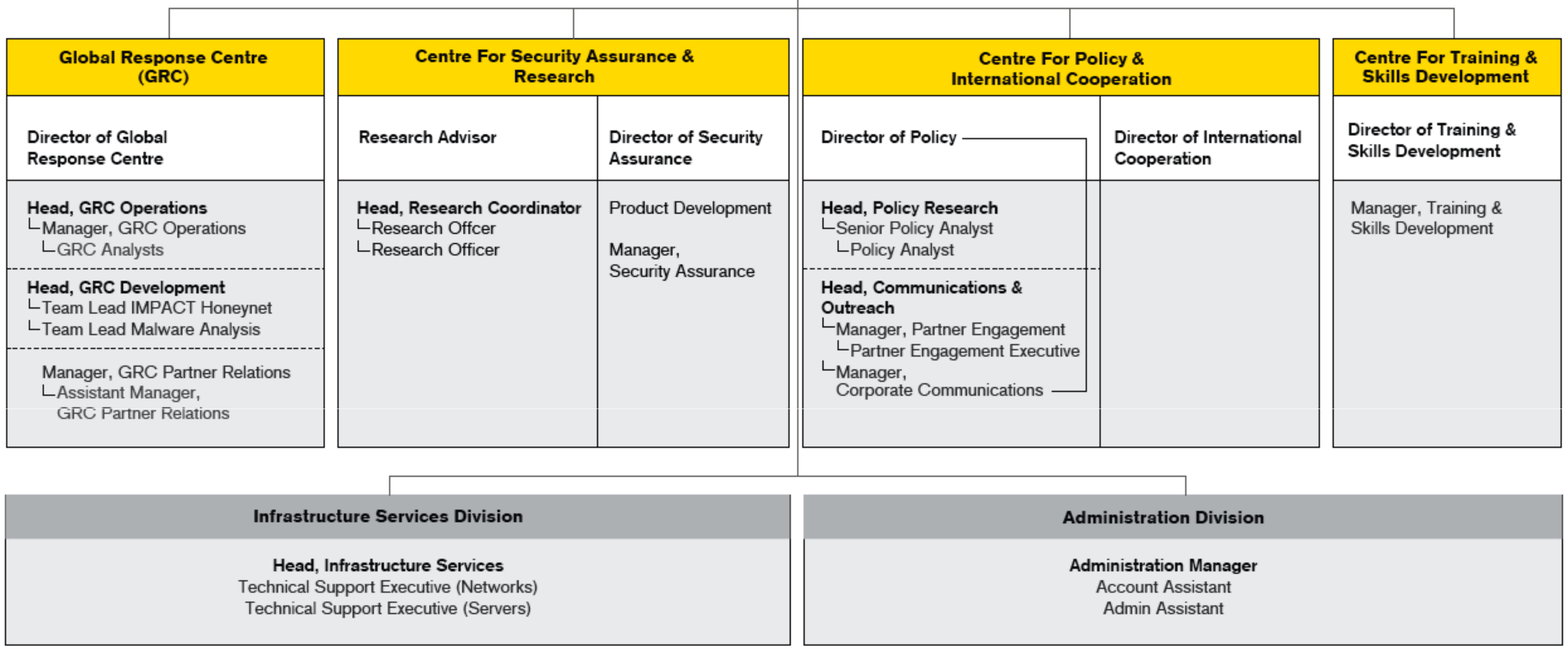
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

International Advisory Board

Management Board
Chairman

Advisor (Technical)

Advisor (Administration)



Global Response Centre (GRC)

Director of Global Response Centre

Head, GRC Operations
└Manager, GRC Operations
└GRC Analysts

Head, GRC Development
└Team Lead IMPACT Honeynet
└Team Lead Malware Analysis

Manager, GRC Partner Relations
└Assistant Manager,
GRC Partner Relations

Centre For Security Assurance & Research

Research Advisor

Head, Research Coordinator
└Research Offcer
└Research Officer

Director of Security Assurance

Product Development

Manager,
Security Assurance

Centre For Policy & International Cooperation

Director of Policy

Head, Policy Research
└Senior Policy Analyst
└Policy Analyst

Head, Communications & Outreach
└Manager, Partner Engagement
└Partner Engagement Executive
└Manager,
Corporate Communications

Director of International Cooperation

Centre For Training & Skills Development

Director of Training & Skills Development

Manager, Training &
Skills Development

Infrastructure Services Division

Head, Infrastructure Services
Technical Support Executive (Networks)
Technical Support Executive (Servers)

Administration Division

Administration Manager
Account Assistant
Admin Assistant

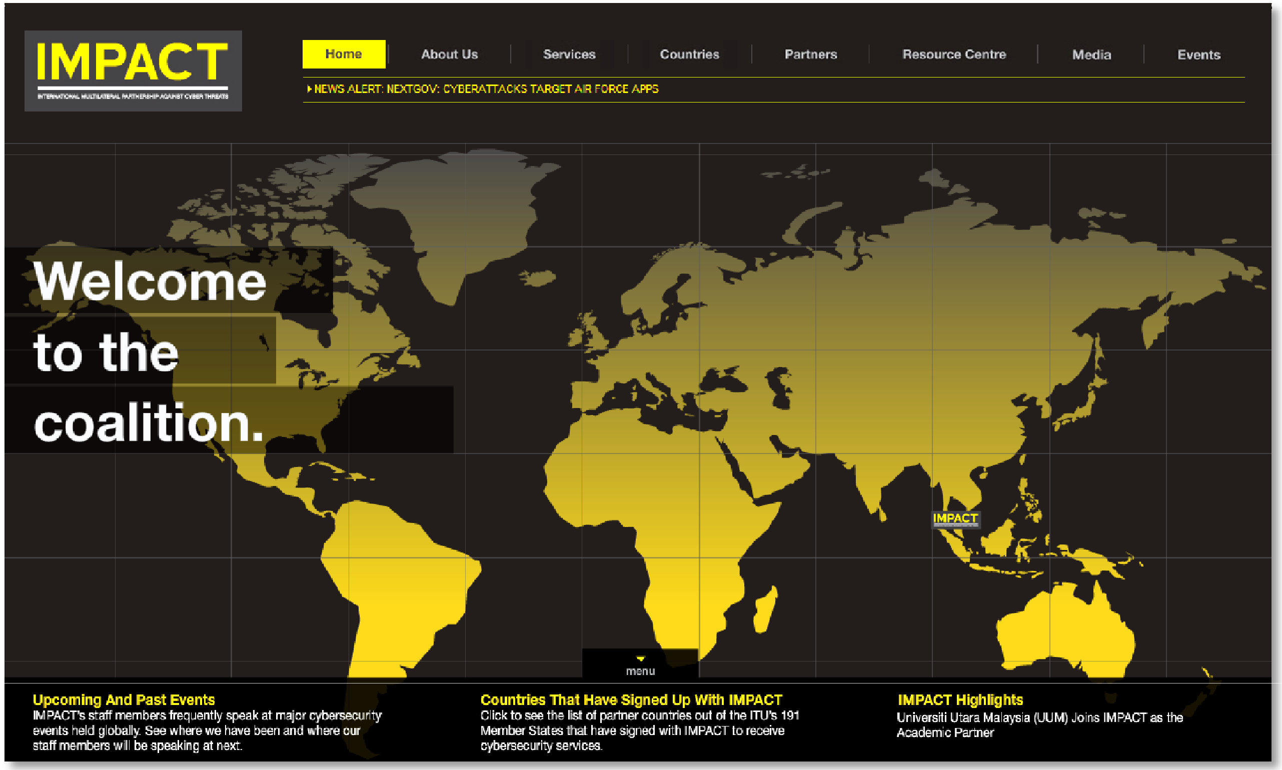
University of Technology, Jamaica

ITU Centres of Excellence Network for the Caribbean Region
Cybersecurity Technologies, Standards & Operations
16-17 September, Kingston, Jamaica

International Telecommunication Union
Committed to connecting the world

IMPACT : Worldwide Alliance

IMPACT International Partners: ITU, UN, INTERPOL and CTO



NEWS ALERT: NEXTGOV: CYBERATTACKS TARGET AIR FORCE APPS

Welcome to the coalition.

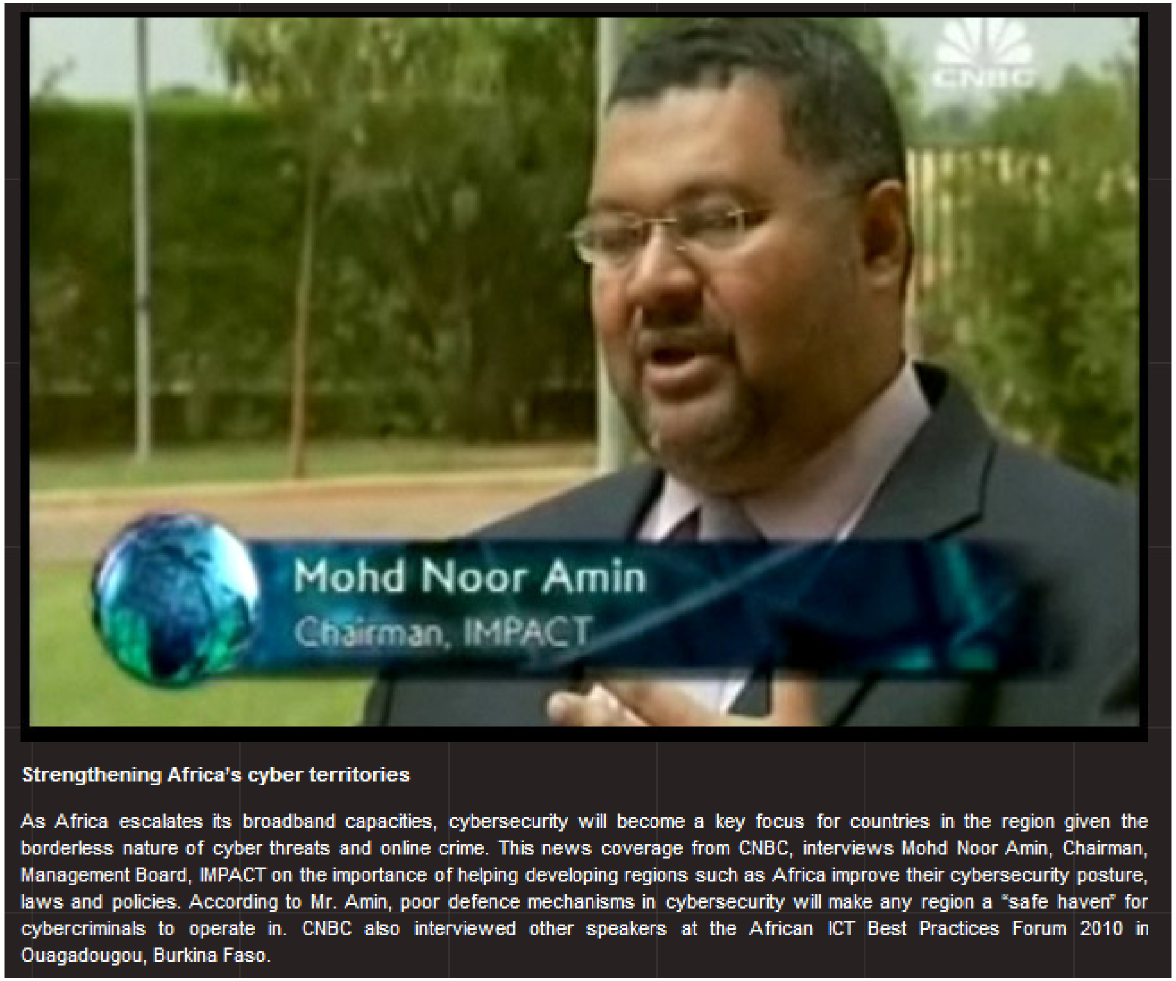
Upcoming And Past Events
IMPACT's staff members frequently speak at major cybersecurity events held globally. See where we have been and where our staff members will be speaking at next.

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

Video: "IMPACT Programmes for AFRICA's Cyber Territories"



Strengthening Africa's cyber territories

As Africa escalates its broadband capacities, cybersecurity will become a key focus for countries in the region given the borderless nature of cyber threats and online crime. This news coverage from CNBC, interviews Mohd Noor Amin, Chairman, Management Board, IMPACT on the importance of helping developing regions such as Africa improve their cybersecurity posture, laws and policies. According to Mr. Amin, poor defence mechanisms in cybersecurity will make any region a "safe haven" for cybercriminals to operate in. CNBC also interviewed other speakers at the African ICT Best Practices Forum 2010 in Ouagadougou, Burkina Faso.

Link : www.impact-alliance.org/resource_centre_multimedia.html

* Workshop Session 6 *

Organising a National Cybercrime Unit (NCU) and National CERT/CSIRT

1–Special Cyber Organisations	2 – CERT/CSIRT Organisation	3 – CERT/CSIRT Alert Centre
4 – CERT/CSIRT: Roll-Out Plan	5 – National Cybercrime Unit	6 – National Cybercrime Unit
7 – ITU: IMPACT Programme	8 – ITU: IMPACT Programme	9 –"Best Practice" for Jamaica

ITU : IMPACT Programme (B)

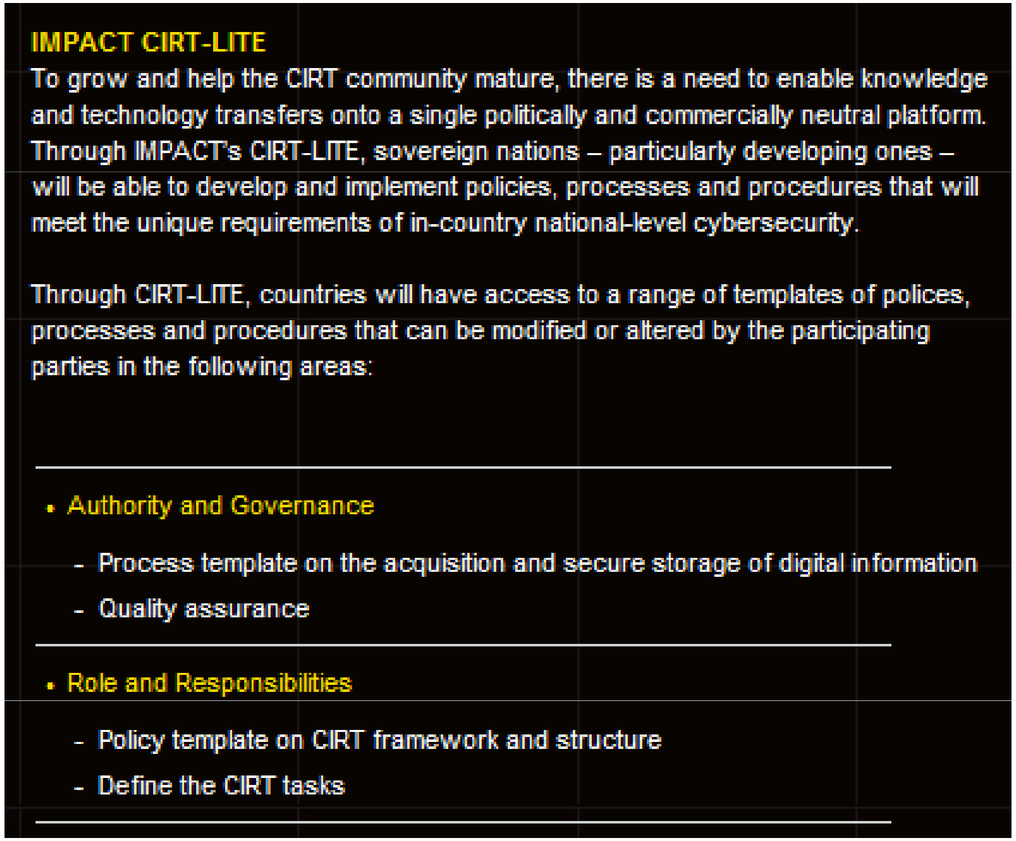
- *IMPACT* is an outstanding example of the 1st New Generation 21stCentury Worldwide *PPP* Organisation that is dedicated to the challenge of tackling global Cyberthreats, Cybercrimes, Cyberattacks and Cyberterrorism

- *The ITU* is promoting the IMPACT Programmes which allow smaller developing countries access to scarce cyber skills and resources especially in areas such as the establishment of CERT/CSIRTs

- The IMPACT – *NEWS Service*: Network Early Warning System – allows countries to gain real-time access to the latest cyber developments malware, threats, attacks, and hence to anticipate and take action with regards to their own national critical information infrastructure

- The IMPACT – *ESCAPE Service*: Electronically Secure Collaboration Platform for Experts – allows real-time collaboration and consultation between experts during the time of massive cyberthreats & crises

IMPACT: CERT/CIRT-LITE Programme

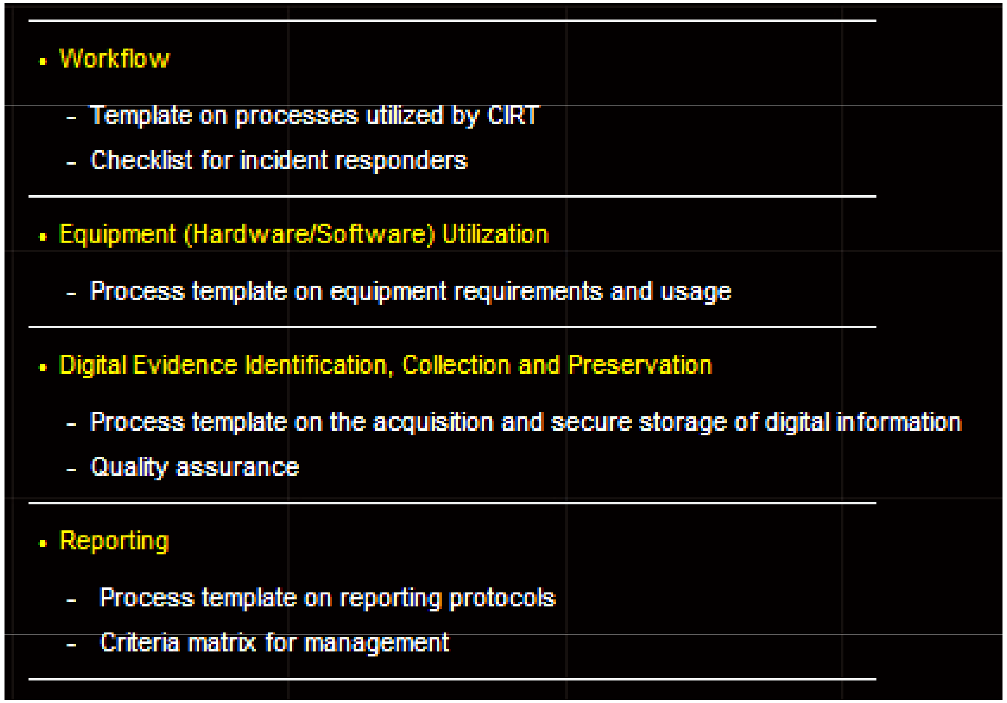


IMPACT CIRT-LITE

To grow and help the CIRT community mature, there is a need to enable knowledge and technology transfers onto a single politically and commercially neutral platform. Through IMPACT's CIRT-LITE, sovereign nations – particularly developing ones – will be able to develop and implement policies, processes and procedures that will meet the unique requirements of in-country national-level cybersecurity.

Through CIRT-LITE, countries will have access to a range of templates of polices, processes and procedures that can be modified or altered by the participating parties in the following areas:

- Authority and Governance
  - Process template on the acquisition and secure storage of digital information
  - Quality assurance
- Role and Responsibilities
  - Policy template on CIRT framework and structure
  - Define the CIRT tasks



- Workflow
  - Template on processes utilized by CIRT
  - Checklist for incident responders
- Equipment (Hardware/Software) Utilization
  - Process template on equipment requirements and usage
- Digital Evidence Identification, Collection and Preservation
  - Process template on the acquisition and secure storage of digital information
  - Quality assurance
- Reporting
  - Process template on reporting protocols
  - Criteria matrix for management

IGSS–Government Security Scorecard Project

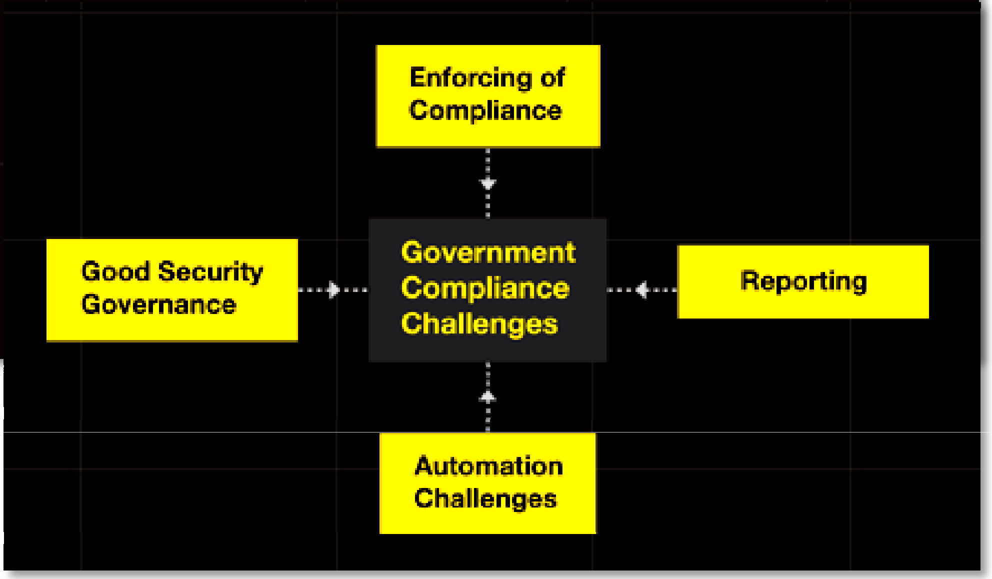
In today's high-tech and interconnected world, a detailed and accurate security governance programme for the public sector is essential. One of the main elements of an effective security programme is the development and enforcement of security policies. This requires the preparation of appropriate reports which can oversee the overall security compliance status of government's vital ministries and agencies on a single dashboard. While governments have cybersecurity policies as part of their security measures, the enforcement of policy compliance has always been a daunting challenge.

In order tighten and achieve compliance, a total automated solution, such as the IMPACT Government Security Scorecard (IGSS) is needed.

Through a centralised and automated analysis of a government's critical business applications and infrastructure, authorised personnel can effectively manage risks by identifying weaknesses and measuring compliance with security practices and regulation requirements. Through its reporting capabilities, IGSS enables the government to understand the critical components of its security postures by analysing compliance at a national-level; this can be filtered down to the region or office level. With IGSS, partner countries will have ONE dashboard view of their security posture and position via an automated audit environment.

IGSS Salient Feature

- Agent-less Architecture
- Platform independent: Works with all the platforms & technologies e.g. Windows, Unix, Linux, Sun.
- All major standards fully built- in: ISO 27001 (ISMS), ISO 25999(Business Continuity Management), Sarbanes-Oxley, GLBA, HIPAA, Basel II, NERC, and FISMA (NIST 800-53).
- Strong Reporting Capability: Comprehensive Dashboard view

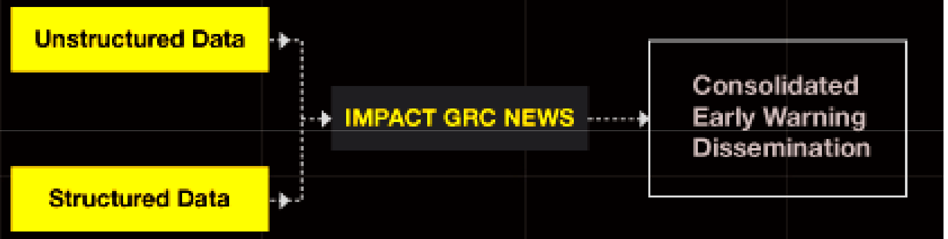


IGSS is currently under development and Malaysia is the first country to adopt this pioneering system

IMPACT GRC: NEWS & ESCAPE Programmes

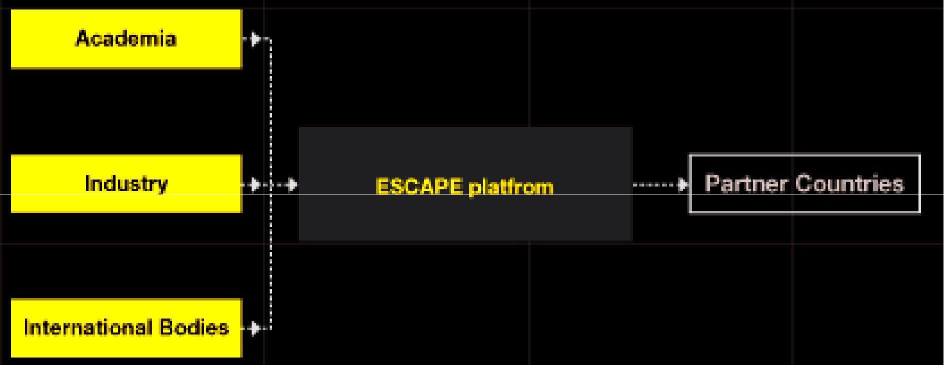
NEWS is a platform of collaborative mashup of information from multiple early warning alliances and cybersecurity vendors. This aims to get the right information to the relevant authorities in a timely manner, enabling them to mitigate and effectively respond to cyber threats that may arise from around the world. Working with leading partners from academia, industry, and international bodies, NEWS provides the global cybersecurity community with real time aggregated early warnings. It also manages the access rights, permissions, information security of the data collected and heightens privacy to sensitive information.

Current leading industry partners in cybersecurity feed the GRC with a tremendous amount of data related to cyber threats, which is disseminated through the NEWS platform thereafter, for remedial in-country action. In addition to the existing providers, GRC – through the NEWS platform – seeks to add more comprehensive data resource providers. With its tremendous amount of cyber threat-related data, NEWS will be the richest knowledge base of its kind in the world.

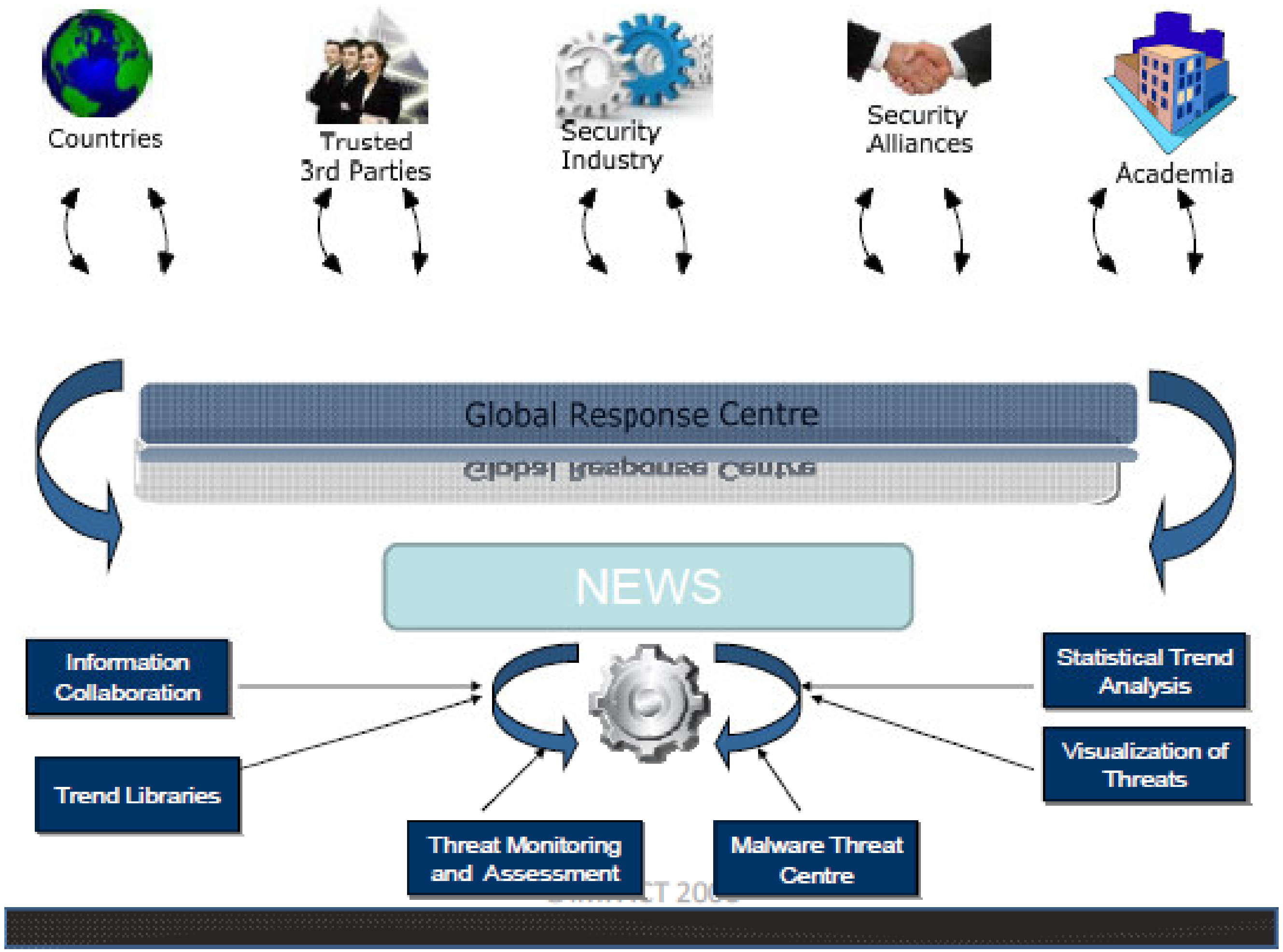


ESCAPE is a tool that allows cybersecurity experts across different countries to pool their resources, share their expertise and remotely collaborate in a secure environment. The ESCAPE platform enables the GRC to act as a one-stop coordination and response centre for countries in times of crisis, enabling the swift identification and sharing of available resources.

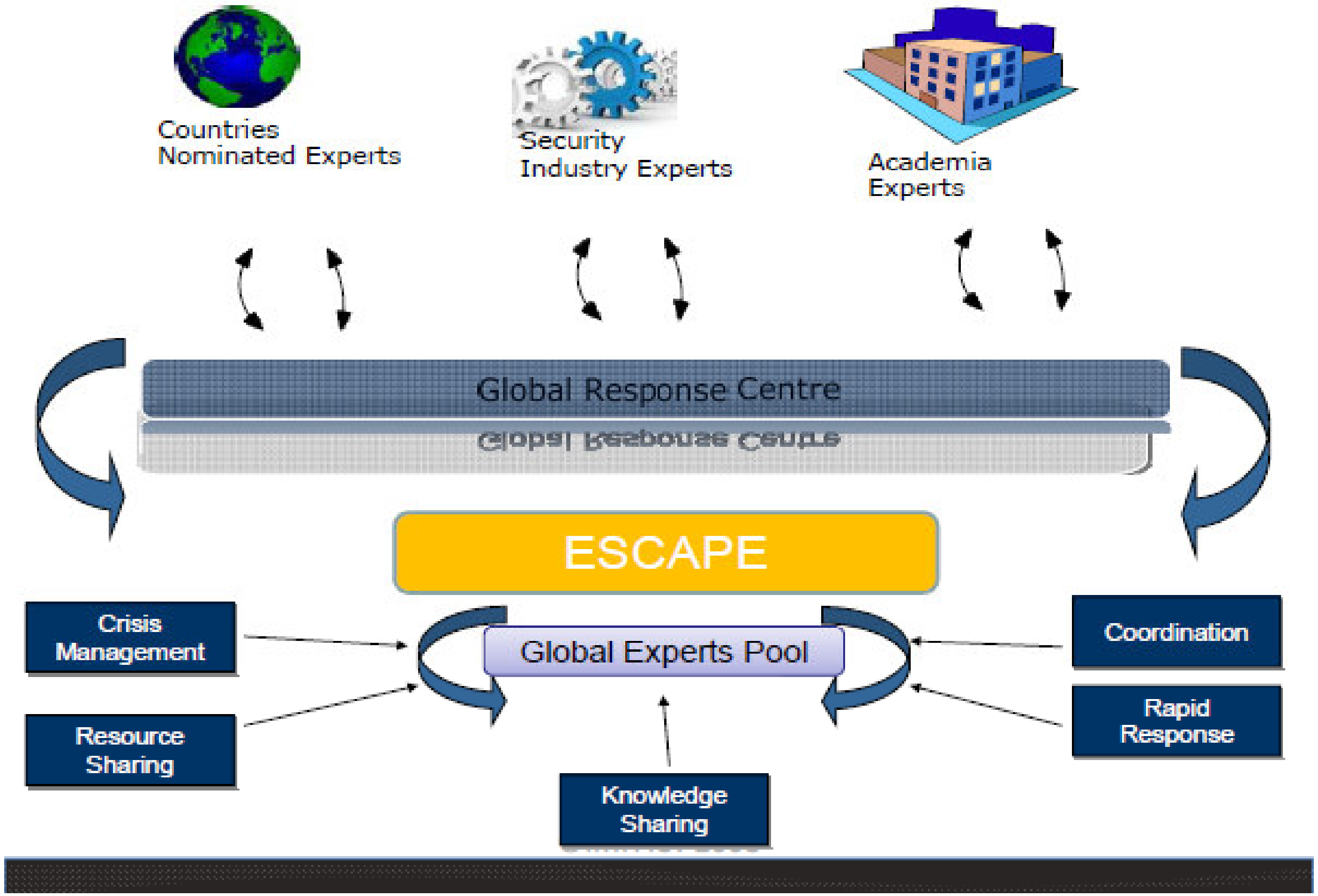
ESCAPE escalates the speed with which IMPACT is able to respond to cyber threats, enabling it to draw from a great pool of talent from across numerous locations. ESCAPE is based on a comprehensive and growing database of key resources around the world which includes IT experts from the industry, authorised national-level personnel such as regulators and other trusted parties that can be called upon in times of need. It provides all the tools and solutions needed to ensure that these individuals and institutions are able to collaborate remotely, securely, and effectively.



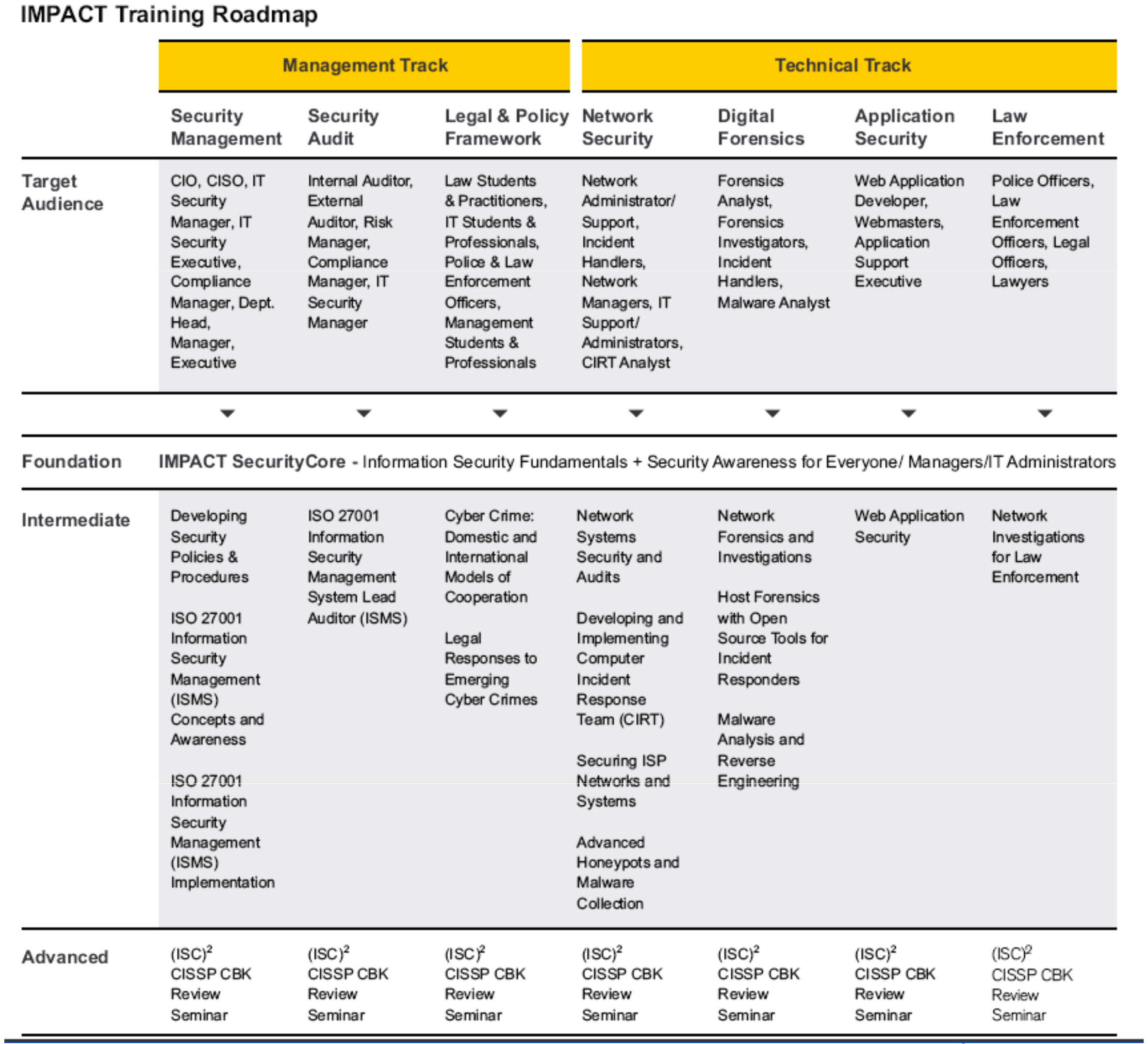
Network Early Warning System(NEWS)



Electronically Secure Collaboration Platform for Experts (ESCAPE)



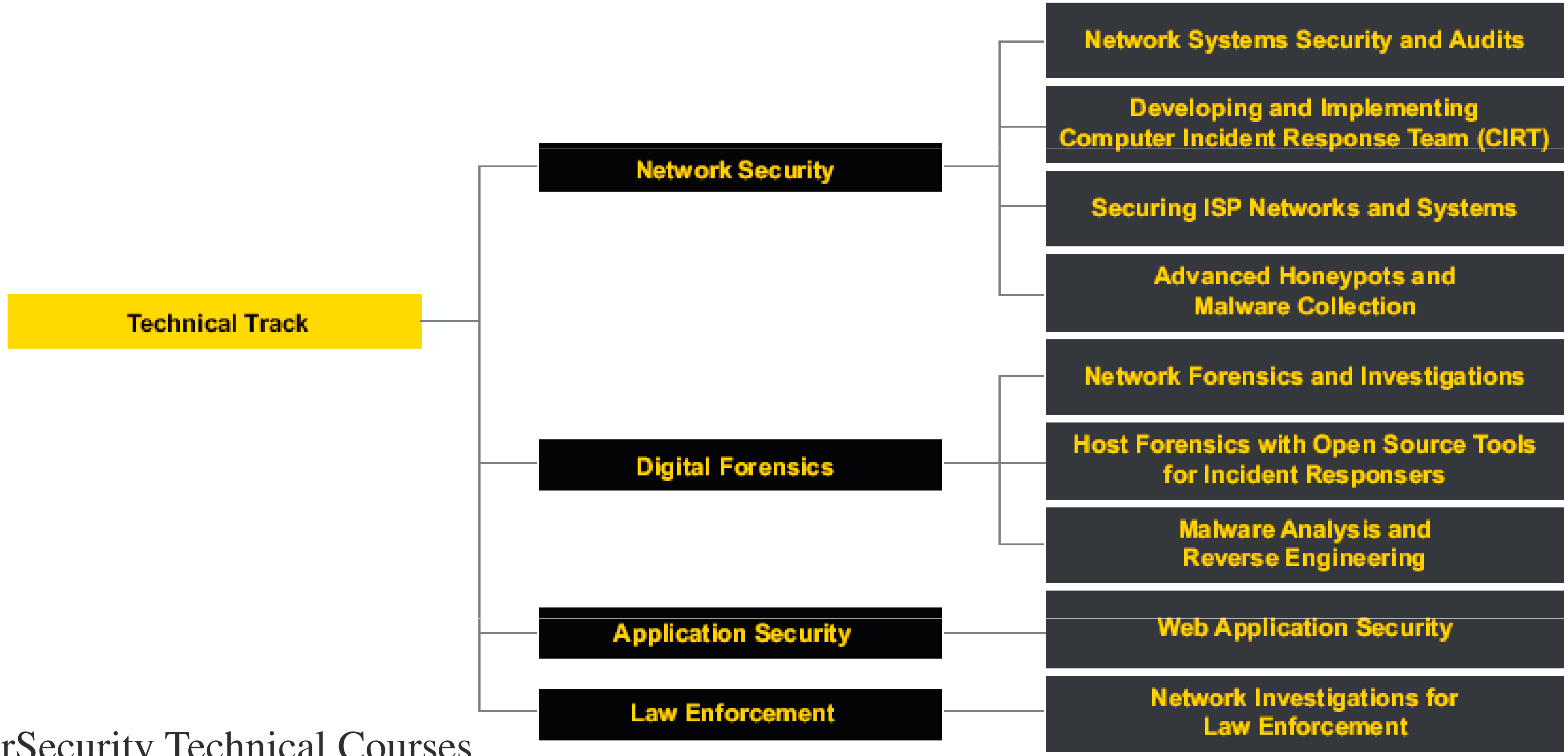
IMPACT: Cyber Training Roadmap



IMPACT Training Roadmap

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

IMPACT: Cybersecurity Technical Training



Technical Track

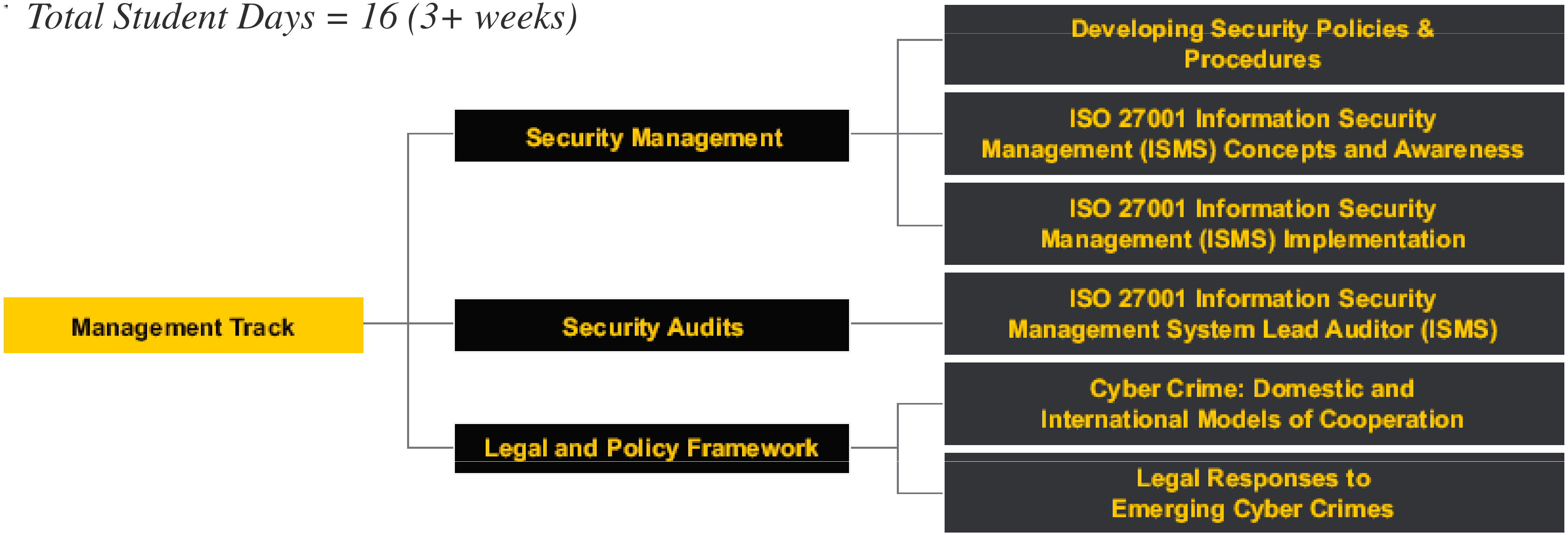
- Network Security
  - Network Systems Security and Audits
  - Developing and Implementing Computer Incident Response Team (CIRT)
  - Securing ISP Networks and Systems
  - Advanced Honeypots and Malware Collection
- Digital Forensics
  - Network Forensics and Investigations
  - Host Forensics with Open Source Tools for Incident Responsers
  - Malware Analysis and Reverse Engineering
- Application Security
  - Web Application Security
- Law Enforcement
  - Network Investigations for Law Enforcement

CyberSecurity Technical Courses
Total Student Days = 41 (8+ Weeks)

IMPACT: Cyber Management Training

CyberSecurity Management Courses

Total Student Days = 16 (3+ weeks)



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

* Workshop Session 6 *

Organising a National Cybercrime Unit (NCU) and National CERT/CSIRT

1–Special Cyber Organisations	2 – CERT/CSIRT Organisation	3 – CERT/CSIRT Alert Centre
4 – CERT/CSIRT: Roll-Out Plan	5 – National Cybercrime Unit	6 – National Cybercrime Unit
7 – ITU: IMPACT Programme	8 – ITU: IMPACT Programme	9 –“Best Practice” for Jamaica

"Best Practice" for Jamaica

- The challenge of "Securing Jamaica" will be a multi-year project as a partnership between Government and Business. Basic principles are:
  - **ITU-GCA:** Structure the programmes using the ITU Global Cybersecurity Agenda
  - **NCA:** Implement Co-ordinating National Cybersecurity Agency with Budget & Authority
  - **Standards:** Adopt and Build to International ITU/ISO Security Standards & Guidelines
  - **Laws:** Check the Jamaican Cybercrimes Act (2009) covers the full spectrum of threats
  - **CERTs:** Establish National Jamaican & Critical Sector Specific CERTs/CSIRTs
  - **eCrimes:** Upgrade and Enhance the Skills and Scope of the JCF-OCID eCrimes Unit
  - **Training:** Organise professional cybersecurity training with certifications

……In-Depth Professional Skills in Cybersecurity Technologies, Standards and Architectures will be mission critical for Jamaican Government & Business to be fully secure in cyberspace!

* ITU Workshop Overview*

“Cybersecurity Technologies, Standards & Operations”

S1-Thurs: 9:30-11:00 “The International Cybercrime and Cybersecurity Challenge”	S2–Thurs:11:30-13:00 “Integration Cyber-Technological Solutions for the 21stC Web2.0 World”	S3-Thurs:14:00-15:30 Group Session: “Securing Critical Computing and Network Facilities”	S4-Thurs:16:00-17:30 Group Session: “Group Discussion: Securing Critical Computing and Network Facilities”
S5 - Fri: 9:30–11:00 “Cybersecurity Continuity Planning, Standards and Architectures”	S6 – Fri: 11:30–13:00 “Organising a National Crime Unit and CERT/CSIRT”	S7 – Fri: 14:00-15:30 Group Session: “Designing Practical Cybercrime Solutions – Critical Sectors”	S7 – Fri: 16:00-17:30 Group Session” “Group Discussion: Designing Practical Cybercrime Solutions – Critical Sectors”

Group Workshop Session 7
"Designing Practical Cybercrime Operation Solutions"

- Task Objective: To select a critical service sector of importance to Jamaica and then to develop a top-level strategy & design is secure against all cybercrime, cyberthreats, cyberterrorism and any other forms of hacking or malicious attack.

  - ***Task 1 –*** Choose your critical sector such as government, banking/finance, telecomms, airports, energy/power, and preferably different from your previous choice in session 3
  - ***Task 2 –*** Consider the scope of your enterprise or agency which may well be multi-site, with national & regional offices, and corresponding ICT networks, databases, facilities and staff
  - ***Task 3 –*** As in session 3, list all the potential cybercrimes, natural disasters and attacks that may threaten your critical sector at either at technical or operational level
  - ***Task 4 –*** Structure your list according to the impact of each potential threat or disaster
  - ***Task 5 –*** Develop a top-level strategy and outline design of your critical sector cybersecurity programme, checking that it provides defence against all the threats you listed in Task 3
  - ***Task 6 –*** Work on a presentation that justifies your critical sector security strategy & design

.....You are the National CIO/CSO for your chosen sector with authority, budget & staff!

* Group Workshop Session 7*
Designing Practical Cybercrime Sector Solutions
Suggested Time Allocations for Task Actions: 90mins

1 – Task Assignment: Choose your Critical Service Sector: ***Government, Banking/Finance Telecomms, Transport, Energy***	**Task 2 – Consider the Scope of your Critical Sector, its multi-site ICT operations & staffing**	**Task 3 – List the Potential Cybercrimes, Cyberthreats, Natural Disasters & Attacks that may threaten the sector**
Task 4 – Structure & Prioritise your list of Cyberthreats	**Task 5 – Develop Top-Level CyberStrategy, Outline Technical & Operational Plan**	**Task 5 – Develop Top-Level CyberStrategy, Outline Technical & Operational Plan**
Task 5 – Check Design against your full List of Cyberthreats	**Task 5 – Prepare Short 10 Min Presentation of Design & Plan**	**Task 5 – Prepare Short 10min Presentation of Design & Plan**

Note: ***Each Task Time Segment = 10Mins***

Task Description: Government Sector

1) You have just been appointed as the new CSO (Chief Security Officer) for the Government working within the Prime Minister's Cabinet Office with top-level responsibility for cybersecurity across all aspects of Government.

2) Your task is to prepare a report & short presentation to the Cabinet regarding the technical and operational actions that should be taken across Government in order to provide an adequate defence against cyberthreats & potential attacks.

3) Assume that the Government comprises around 20 Ministries including Foreign Office, Home Office, Security, Defence, Transportation, Finance, Justice, Energy, Environment, Healthcare and Industry, as well as Regional Administrations

4) There is already a Government Data Network and various ICT computer centres and databases that are not yet secured against cyber threats & attacks

…..Plan your security priorities, and prepare a practical cybersecurity action plan

Task Description: Banking/Finance Sector

1) You have just been appointed as the CSO (Chief Security Officer) for a major National Financial Institution with both retail & investment operations

2) Your task is to prepare a report and presentation for the Board of Management with recommendations on the technical and operational actions that should be taken across the Financial Group to provide security against cybercriminal attacks

3) Assume that the Bank includes a large national retail network of local branches and ATM machines, as well as on-line banking operations. Also assume that the investment banking operations are networked with several other major global banking networks and that stocks, bonds & commodities are traded in real-time

4) There have already been cybercriminal attacks on bank accounts & transactions in the past year and you are asked by the CEO to ensure that any future attacks are immediately detected, maybe with an in-house CERT, and any losses minimised

……Consider all the potential cyber threats and prioritise your action plan for the Board

Task Description: Telecomms/Mobile Sector

- You have just been appointed as the CSO (Chief Security Officer) for the National Telecommunications or Mobile Networking Carrier in Jamaica

- Your task is to prepare a full report and presentation to your Board of Management with recommendations for upgrading all aspects of cybersecurity, specifically focusing upon the technical and operational procedures & measures

- Assume that the National Telecomms and/or Mobile Operations comprises a national distributed radio and landline network with a range of traditional telecomms and broadband "new generation" IP technology switches & servers.

- You are responsible for ALL aspects of network security including the private leased line (VPN) networks for the government & large enterprises, as well as the telecomms ISP operations which includes Hosted eCommerce WebSites, VoIP & Gateways & Routers to other Regional and International Networks

…Consider all the threats and prioritise your actions in order to minimise the risks and potential damage from future cyber attacks on the national telco network

Task Description: Transport/Airports Sector

- You have just been appointed the CSO (Chief Security Officer) for the country's largest international airport (Kingston), including both passenger and cargo operations, as well as associated regional airports (Montego Bay)

- Your task is to prepare a report and presentation to the Board of Management for the Airport with recommendations and action plan for the upgrading of all aspects of security across the airport/port operational and ICT facilities.

- Assume that the Airport has both airside and landside operations, with multiple domestic and international airlines flying routes to an intensive schedule. The ICT assets include the real-time air traffic control, passenger & cargo screening systems, staff and vehicle access, and the computerised dispatching network and baggage handling network.

- You are responsible as CSO for both the operational security and associated security staff as well as all the cybersecurity aspects of the airport operation.

…Consider all the possible cybercriminal and cyberterrorist threats to the airport facilities and prioritise your action plan to minimise risks from potential attacks

Task Description: Energy/Utilities Sector

- You have recently been appointed as the CSO (Chief Security Officer) for the National Energy and Power Grid which provides most of the nation's energy

- Your task is to prepare a report and presentation for the Board of Management with recommendations and action plan for upgrading all aspects of security with respect to the National Power Grid and its regional centres and operations

- Assume that the National Power Grid and Company has several large power stations (non-nuclear) and distribution network across cities, towns & villages. The ICT computer facilities include all the power station process control networks & applications, as well as the 24/7 real-time management of energy (electricity & gas flow) through the national power grid to business & end-users

- You are responsible as CSO for both the technical aspects of ICT cybersecurity as well as operational security for the power stations, offices and other facilities

….Consider all the possible cyberthreats and cyberterrorism that could impact the national grid and prioritise a practical plan that minimises the risk of attack, and reduces the collateral damage and disruption following any major power failure

Key to Cybersecurity Workshop Session Colour-Code Classifications: Interactive Tasks

Colour Code Workshop	RED	ORANGE	YELLOW	BLUE	GREEN
Monday ***-Action Plans -***	(1) Legal	(2) Technical	(3) Organisation	(4) Capacity	(5) International
Tuesday ***- Laws -***	Information Disclosure	Computer Misuse	Forgery & ID Fraud	Information Interception	Copyright & Patents Law
Wednesday ***- Road Map -***	Q1-2011	Q2-2011	Q3-2011	Q4-2011	FY2012
Thursday ***- ICT Security-***	Unauthorised Info Access	DDoS-Denial of Services	MALWARE	Disclosure & Misuse	Info Access & Exploitation
Friday ***- Sector Security -***	**Cyber Criminal Threat**	**Cyber Terrorist Threat**	**Malicious Hacking & Exploitation**	**Internal Operational Threat**	**Natural Disaster or Other Event**

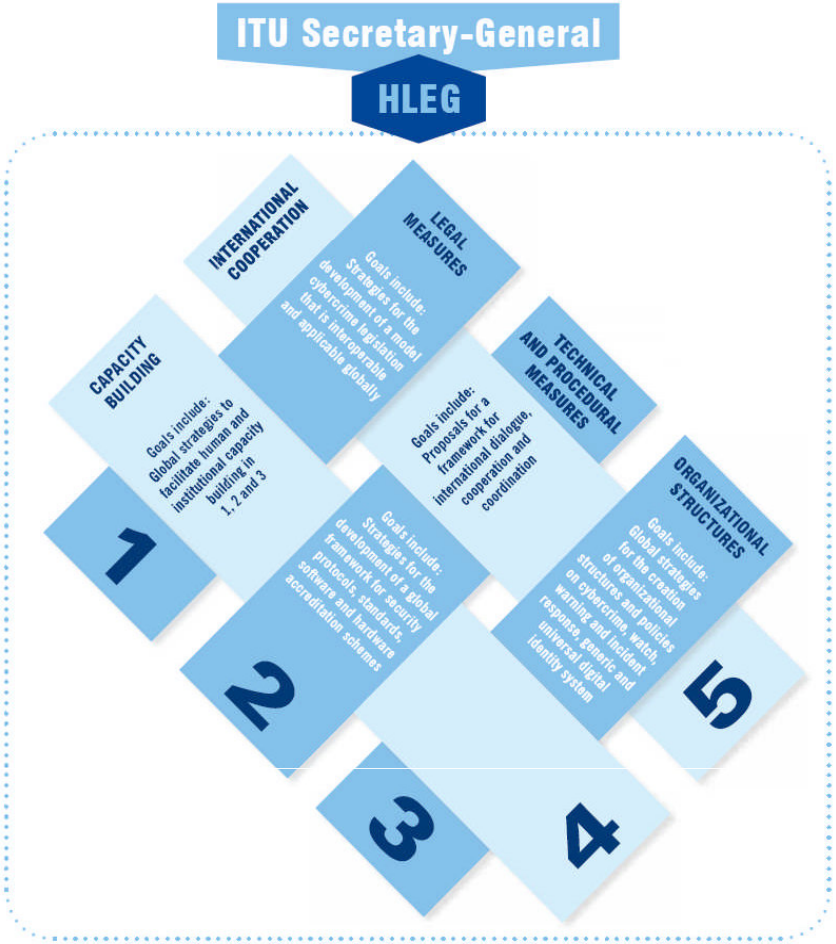
* ITU Workshop Overview*

“Cybersecurity Technologies, Standards & Operations”

S1-Thurs: 9:30-11:00 “The International Cybercrime and Cybersecurity Challenge”	S2–Thurs:11:30-13:00 “Integration Cyber-Technological Solutions for the 21stC Web2.0 World”	S3-Thurs:14:00-15:30 Group Session: “Securing Critical Computing and Network Facilities”	S4-Thurs:16:00-17:30 Group Session: “Group Discussion: Securing Critical Computing and Network Facilities”
S5 - Fri: 9:30–11:00 “Cybersecurity Continuity Planning, Standards and Architectures”	S6 – Fri: 11:30–13:00 “Organising a National Crime Unit and CERT/CSIRT”	S7 – Fri: 14:00-15:30 Group Session: “Designing Practical Cybercrime Solutions – Critical Sectors”	S7 – Fri: 16:00-17:30 Group Session” “Group Discussion: Designing Practical Cybercrime Solutions – Critical Sectors”

GLOBAL CYBERSECURITY AGENDA

A FIVE-PART PLATFORM



ITU Secretary-General

HLEG

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

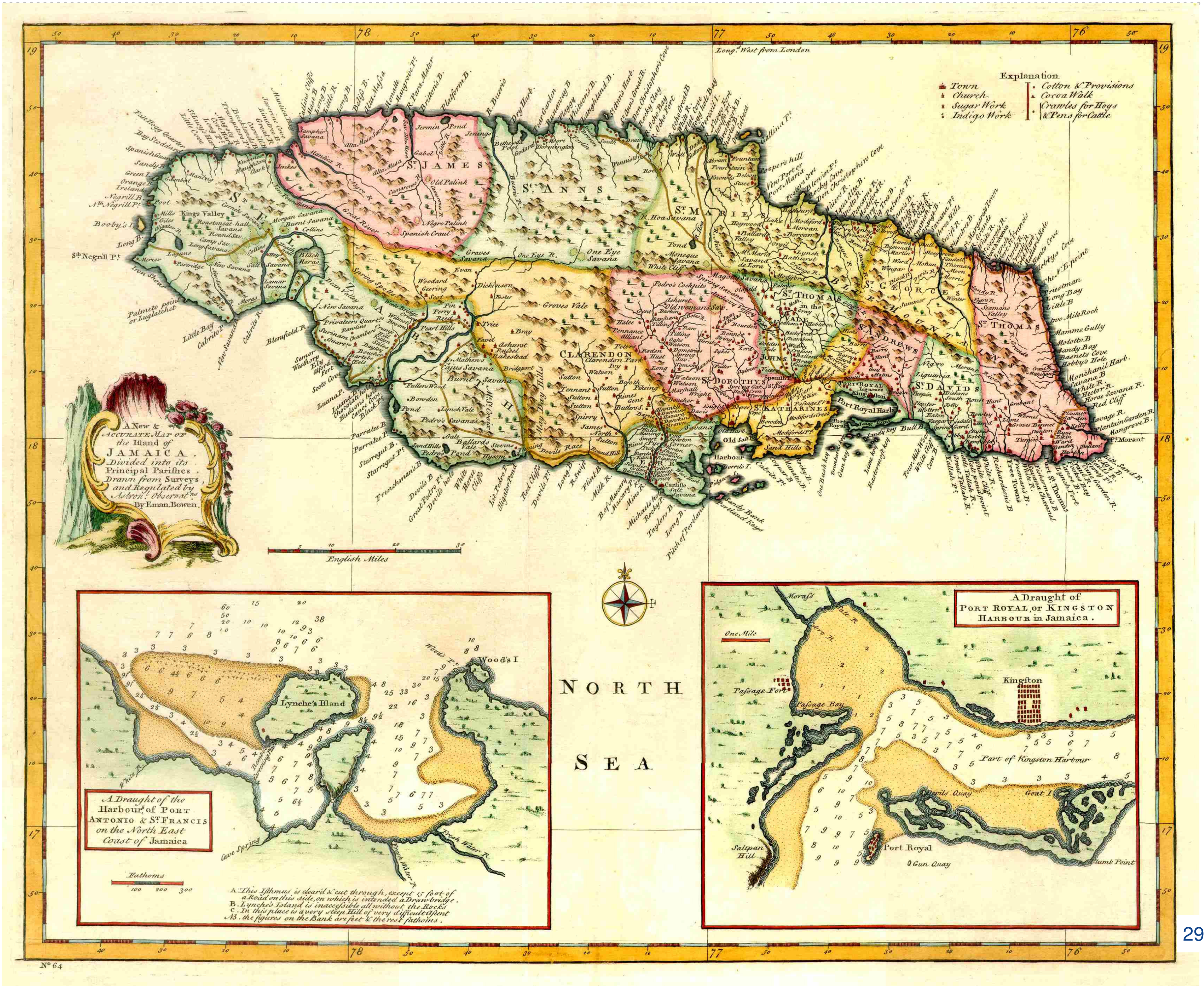
Goals include: Proposals for a framework for international dialogue, cooperation and coordination

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

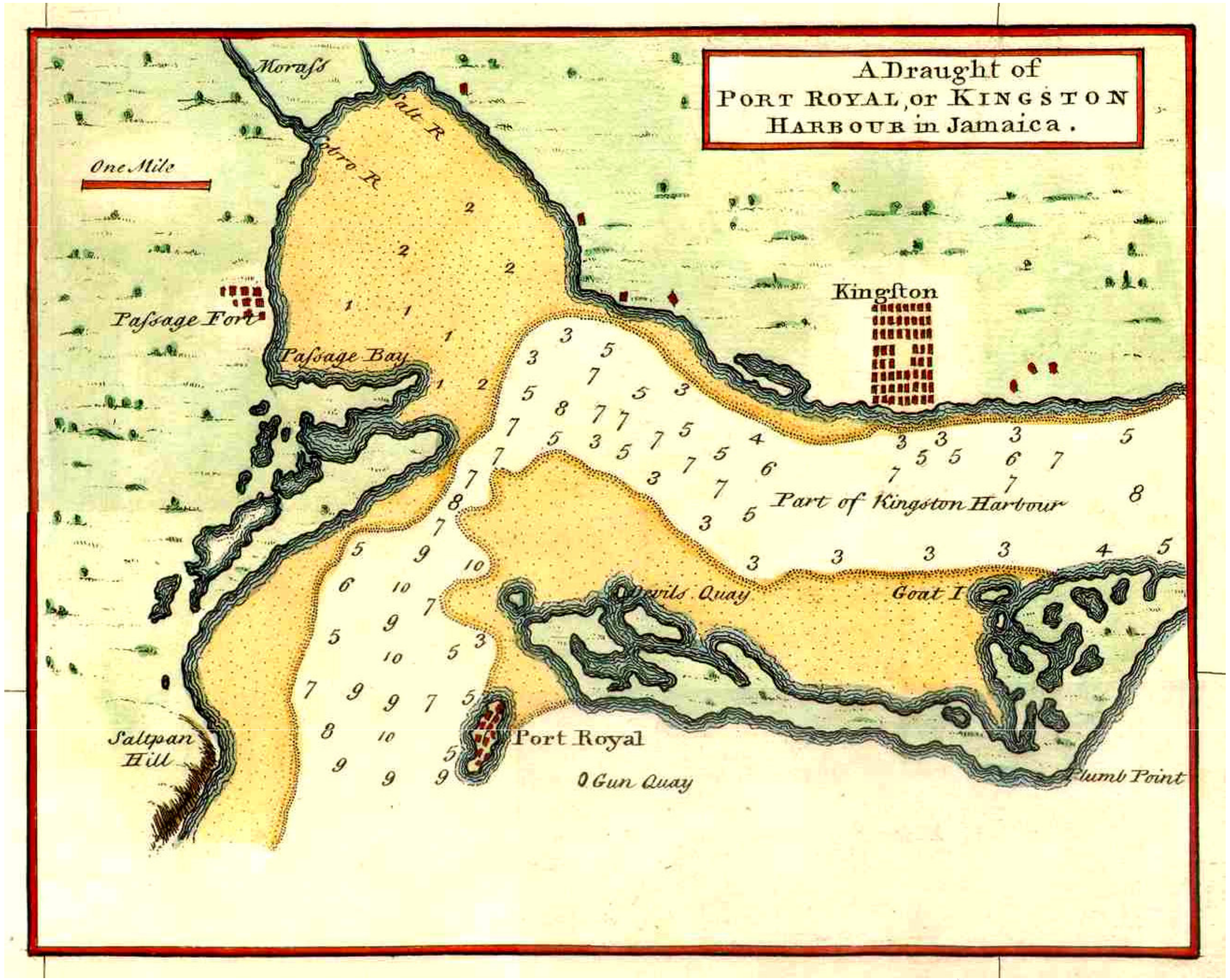
ORGANIZATIONAL STRUCTURES

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

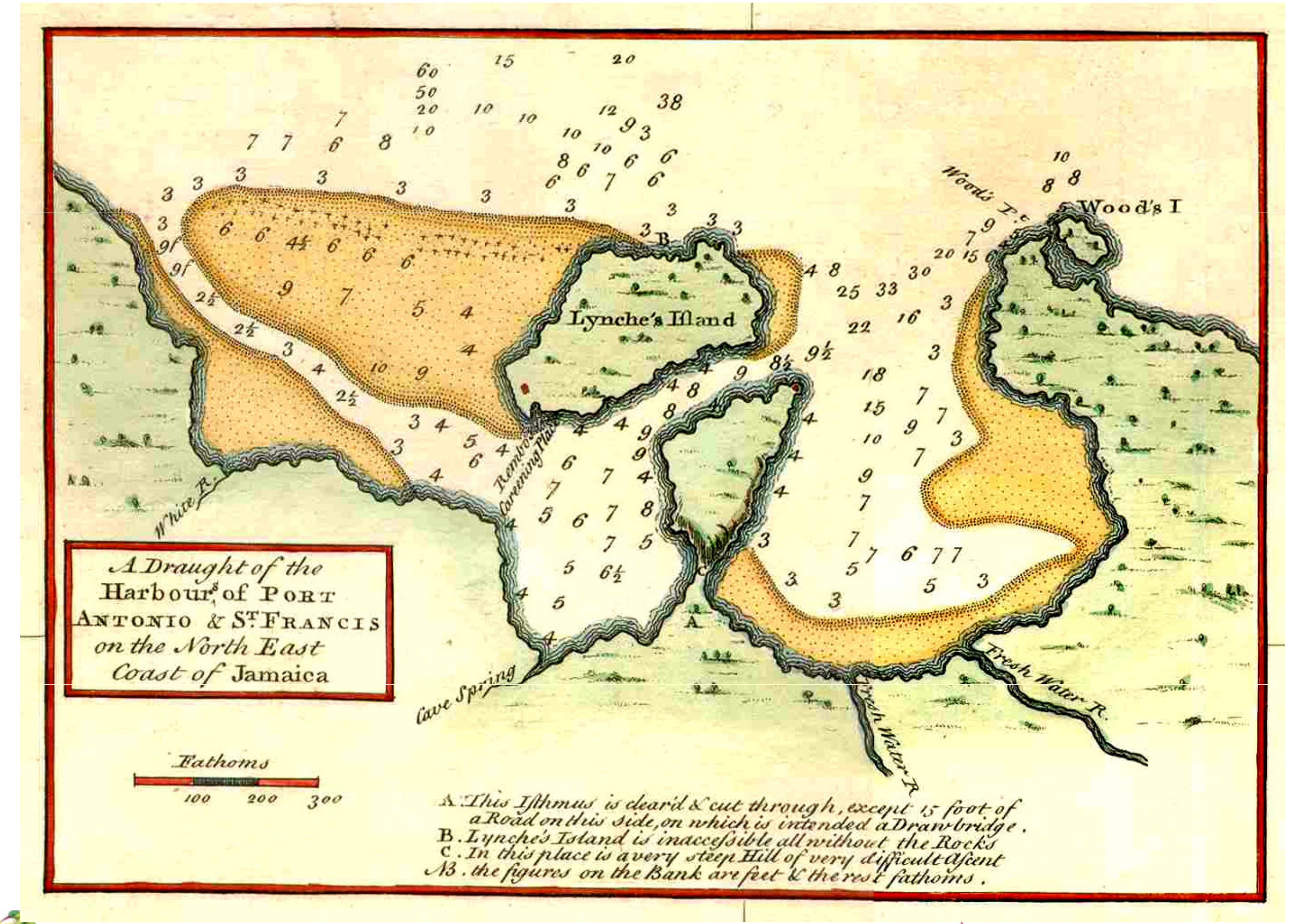
Securing the Island of Jamaica for 260 Years: 1750 to 2010


A New & ACCURATE MAP OF the Iſland of JAMAICA. Divided into its Principal Pariſhes. Drawn from Surveys, and Regulated by Astron.l Observat.ns By Eman. Bowen.
Long.e West from London
Explanation
Town
Church
Sugar Work
Indigo Work
Cotton & Provisions
Cocoa Walk
Crawles for Hogs & Pens for Cattle
St. JAMES
St. ANNS
St. MARIES
St. GEORGES
St. THOMAS
St. ANDREWS
St. DAVIDS
St. THOMAS in the VALE
St. JOHNS
St. DOROTHYS
St. KATHARINES
CLARENDON
VERE
St. ELIZABETH
HANOVER
WESTMORELAND
BLUE MOUNTAINS
Port Royal
Port Royal Harb.
Kingston
Old Harb.
Pt. Morant
Sth. Negrill Pt.
English Miles
NORTH SEA
A Draught of the Harbour of PORT ANTONIO & St. FRANCIS on the North East Coast of Jamaica
Lynche's Iſland
Wood's I
Cave Spring
Fresh Water R.
Fathoms
A. This Iſthmus is clear'd & cut through, except 15 foot of a Road on this side, on which is intended a Drawbridge.
B. Lynche's Island is inacceſsible all without the Rocks
C. In this place is a very steep Hill of very difficult Aſcent
NB. the figures on the Bank are feet & the rest fathoms.
A Draught of PORT ROYAL, or KINGSTON HARBOUR in Jamaica.
One Mile
Paſsage Fort
Paſsage Bay
Part of Kingston Harbour
Salt pan Hill
Gun Quay
Goat I.
Plumb Point
No. 64

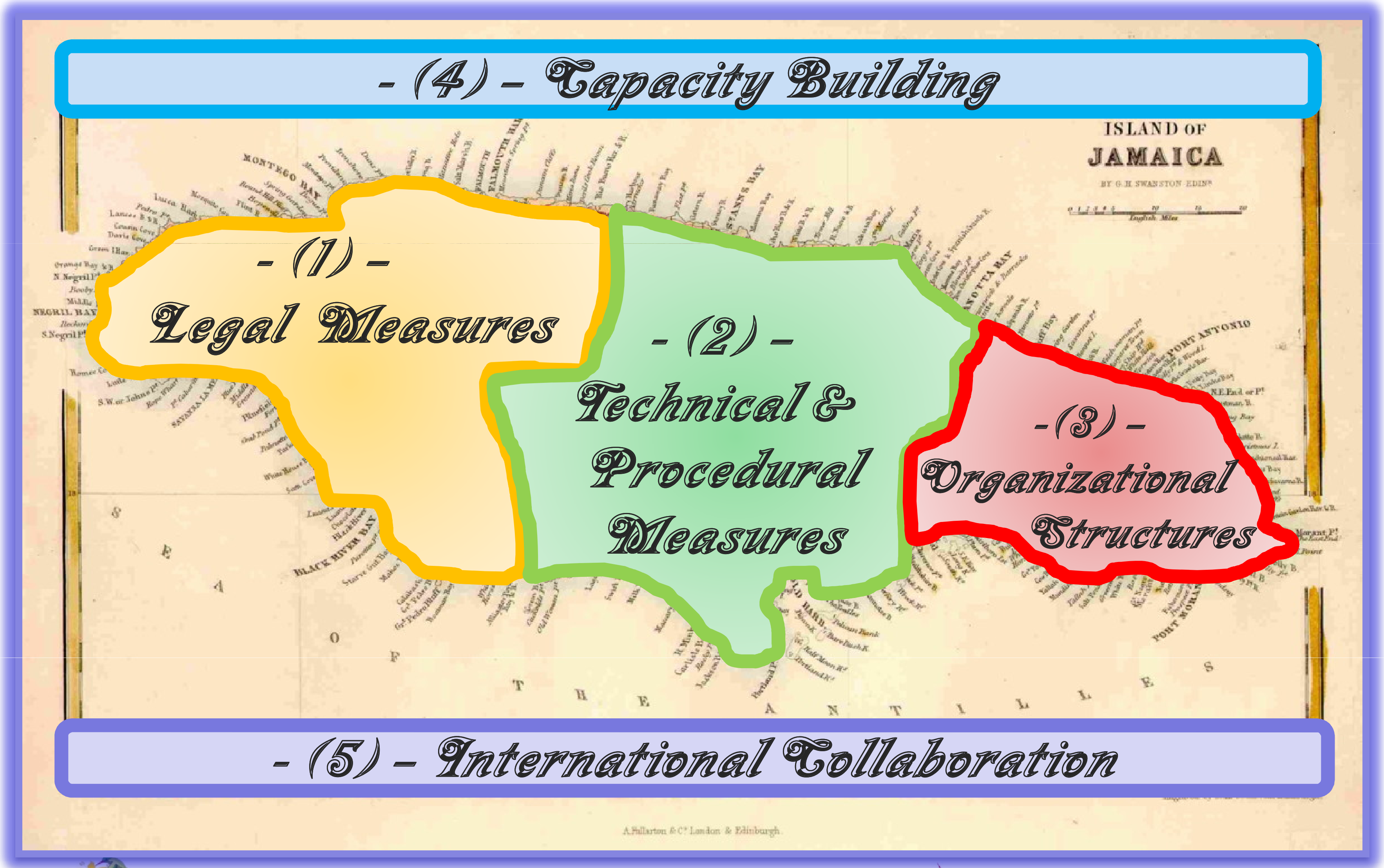
From 18th C Coastal Forts in 1750 to 21st C Cybersecurity in 2010



18thC Coastal Jamaican Ports required Protected Bays for Physical Defence


A Draught of the Harbours of Port Antonio & St. Francis on the North East Coast of Jamaica
Lynche's Iſland
Wood's I
Wood's P.
White R.
Rembro Careening Place
Cave Spring
Fresh Water R.
Fresh Water R.
A
B
Fathoms
100
200
300
A. This Iſthmus is clear'd & cut through, except 15 foot of a Road on this side, on which is intended a Drawbridge.
B. Lynche's Iſland is inacceſsible all without the Rocks
C. In this place is a very steep Hill of very difficult Aſcent
NB. the figures on the Bank are feet & the rest fathoms.

Securing Jamaica in Cyberspace!…
….The Next BIG Strategic Challenge



- (4) – Capacity Building

- (1) – Legal Measures

- (2) – Technical & Procedural Measures

-(3) – Organizational Structures

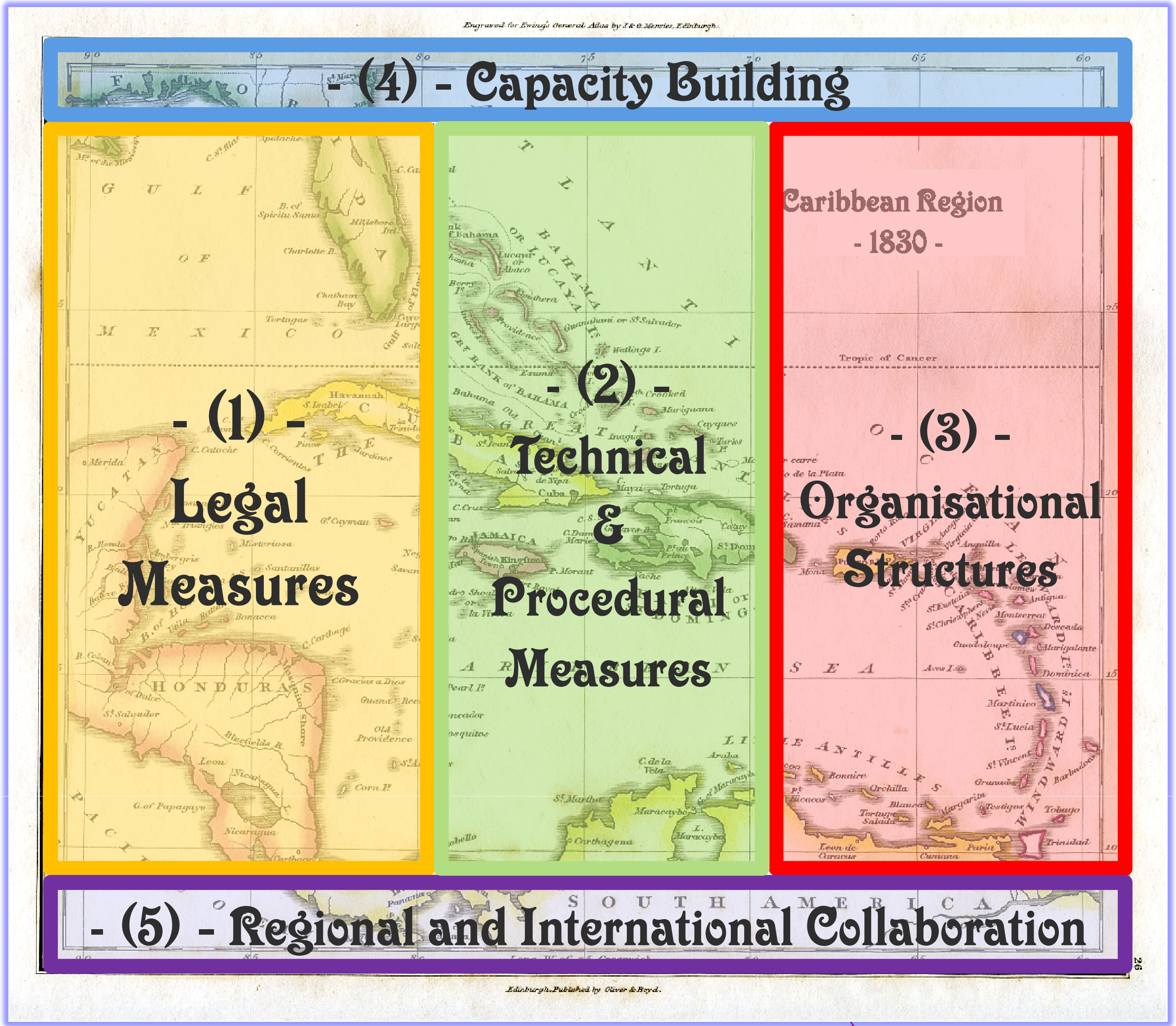
- (5) – International Collaboration

University of Technology, Jamaica

ITU Centres of Excellence Network for the Caribbean Region
Cybersecurity Technologies, Standards & Operations
16-17 September, Kingston, Jamaica

International Telecommunication Union
Committed to connecting the world

Securing the Caribbean in Cyberspace!



- (4) - Capacity Building

- (1) - Legal Measures

- (2) - Technical & Procedural Measures

- (3) - Organisational Structures

- (5) - Regional and International Collaboration

* Group Workshop Session 8*
Team Discussion: Cybercrime Security Operations
Schedule: Task Presentations = 90mins

Group 1 = Government (15mins)

Group 2 = Banking/Finance (15Mins)

Group 3 = Telecomms/Mobile (15Mins)

Group 4 = Transport or Energy (15Mins)

Group Task Discussion (10Mins)

Review On-Line Resources and Next Steps for Personal Study & Research on Cybersecurity

Final Discussion & Wrap-Up

On-Line Cybersecurity Resources

- *ITU Cybersecurity Toolkits*, Reports and Standards
  - ITU Cybercrime Toolkit & Cybercrime Guidelines for Developing Countries
  - ITU Toolkit on "Botnet" Mitigation – *Protection against Denial of Service Attacks*
  - ITU Self-Assessment Toolkit for CIIP – Critical Information Infrastructure Protection
  - ITU Technical Security Standards such as X.800 Series and the X.1200 Series
- *Technical Publications* on Cybersecurity from NIST, ISF, ISO, ENISA well as the Cybersecurity Organisations from national Governments
  - NIST – National Institute of Standards and Technology ("800" Security Series)
  - ENISA – European Network & Information Security Agency
  - ISF – Information Security Forum
  - ISO – International Standards Organisation
- *Industry White Papers* and Reports from the major ICT Cybersecurity Companies such as Symantec, Sophos, Kaspersky Labs and McAfee
- *On-Line "Google" Searches* generate 15Mil+ "hits" from *"cybersecurity"*, whilst a refined search will provide *daily news* updates & *latest reports*

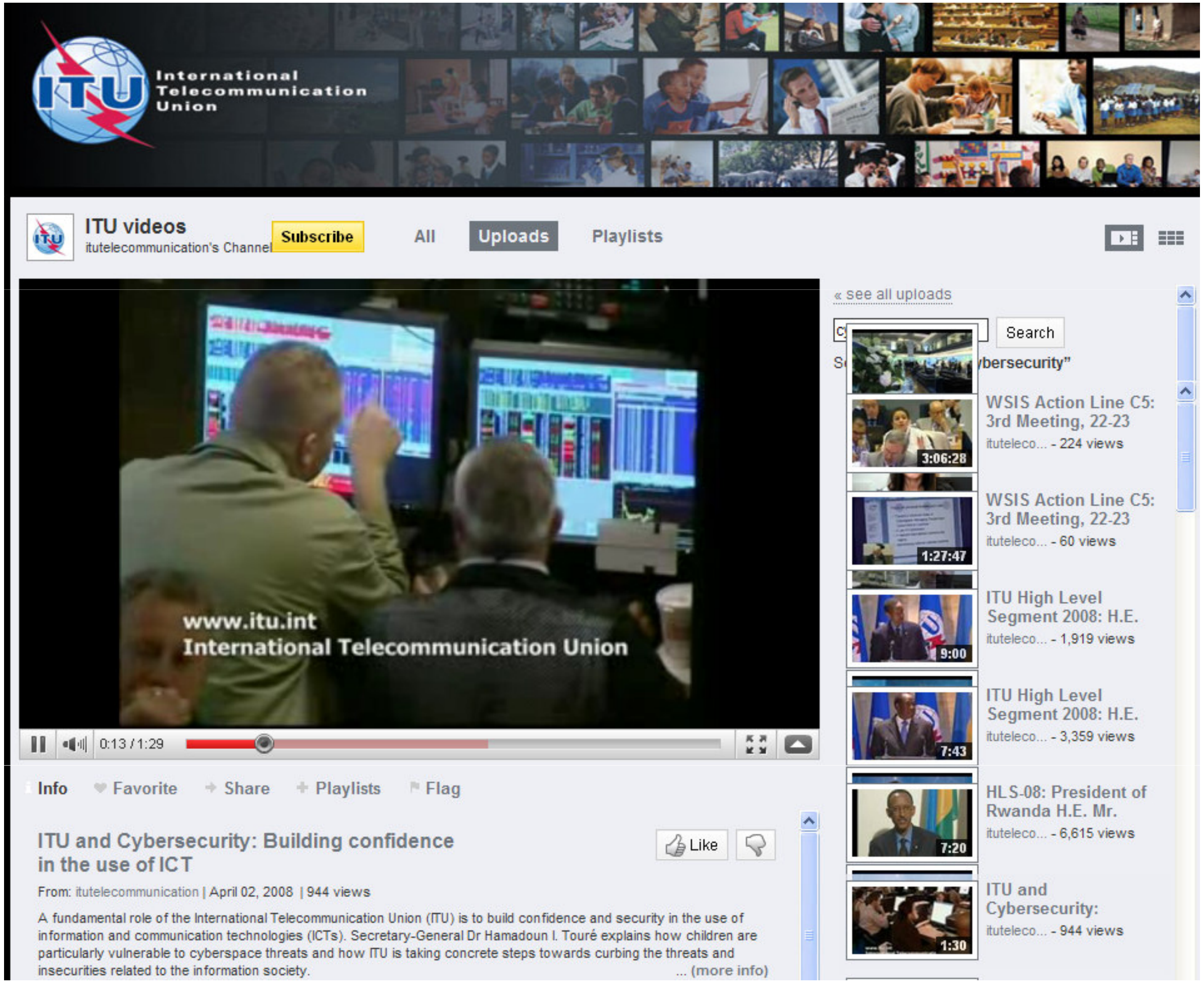
On-Line Cybersecurity Resources: ITU

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

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

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

ITU: On-Line Video Channel – Interviews & Updates



ITU and Cybersecurity: Building confidence in the use of ICT

From: itutelecommunication | April 02, 2008 | 944 views

A fundamental role of the International Telecommunication Union (ITU) is to build confidence and security in the use of information and communication technologies (ICTs). Secretary-General Dr Hamadoun I. Touré explains how children are particularly vulnerable to cyberspace threats and how ITU is taking concrete steps towards curbing the threats and insecurities related to the information society. ... (more info)

3:06:28	WSIS Action Line C5: 3rd Meeting, 22-23 ituteleco... - 224 views
1:27:47	WSIS Action Line C5: 3rd Meeting, 22-23 ituteleco... - 60 views
9:00	ITU High Level Segment 2008: H.E. ituteleco... - 1,919 views
7:43	ITU High Level Segment 2008: H.E. ituteleco... - 3,359 views
7:20	HLS-08: President of Rwanda H.E. Mr. ituteleco... - 6,615 views
1:30	ITU and Cybersecurity: ituteleco... - 944 views

On-Line Cybersecurity Resources: Other

1) UK ACPO Manager's Guide to e-Crime Investigation V1.4 – 2009
2) UK ACPO National e-Crime Strategy – Report 2009
3) UK ACPO Good Practice Guide for Computer-Based Electronic Evidence-2009

………UK eCrime Unit WebLink: www.met.police.uk/pceu

4) Cybersecurity Strategy of the United Kingdom: Cabinet Office – 2009- cabinetoffice.gov.uk
5) Guide to NIST Security Documents: US Dept of Commerce – 2009 - www.csrc.nist.gov
6) ISF (Information Security Forum): Standard of Good Practice for InfoSec – 2007

…….ISF WebLink: www.securityforum.org

7) CMU: Steps for Creating National CSIRTs – Carnegie Mellon Uni – 2004 – www.cert.org
8) ENISA: Step-by-Step Approach on How to Set up a CSIRT – 2006
9) ENISA: CERT Exercise Handbook and Training Handbook – 2008

…….ENISA WebLink: www.enisa.europa.eu/act/cert/

…….Most documents referenced during this ITU Cybersecurity Workshop will be found with a focused Google Search for the Publication Title & Responsible Organisation

Group Workshop Session 8 Discussion: *Designing Practical Cybercrime Operational Solutions*

1) Workgroup Task Cybercrime Presentations

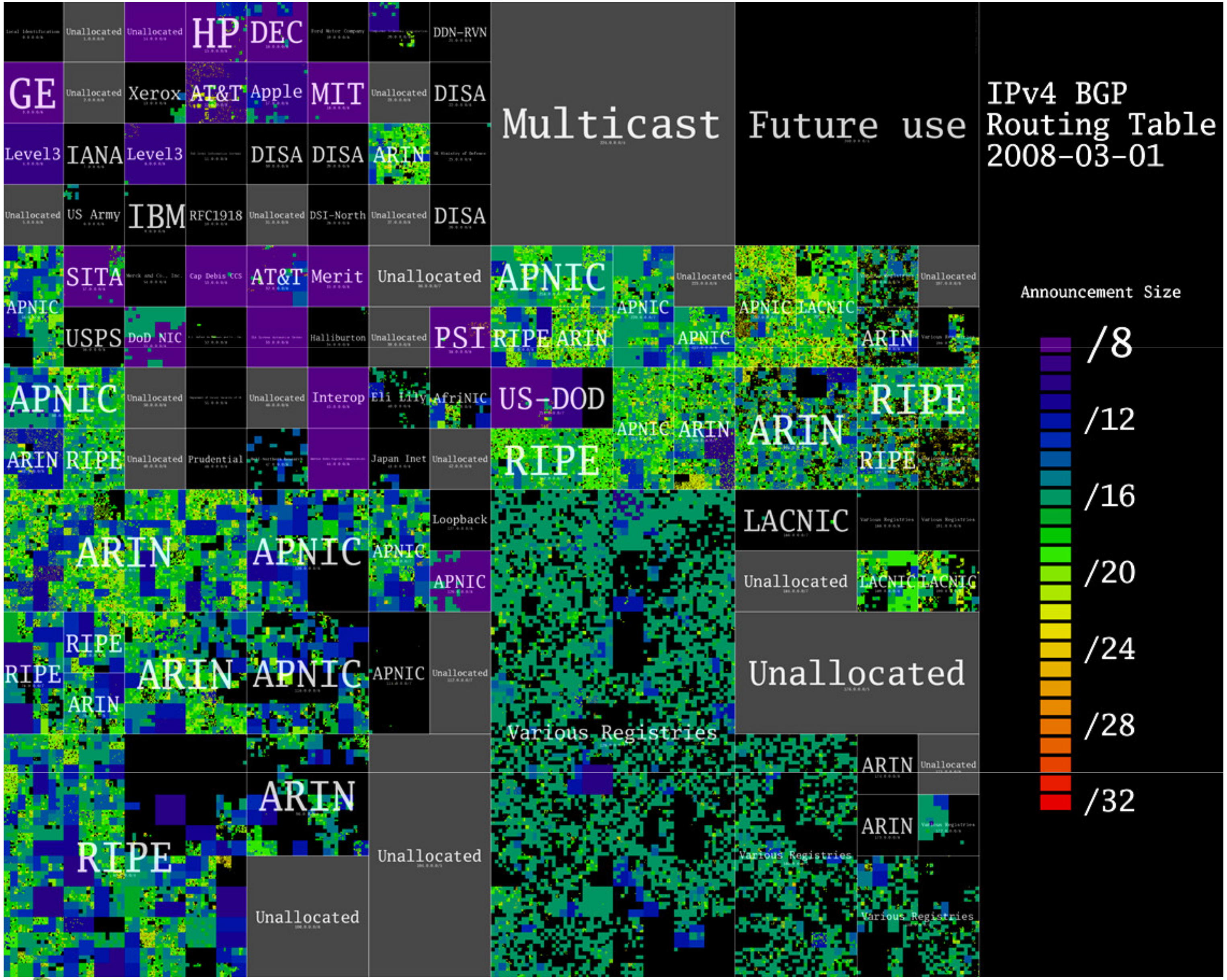
2) Feedback on the Workshop, Content and Tasks

3) Final Questions, Discussion and Wrap-Up!

…Thank-You!

BACK-UP SLIDES

Global IP Map of BGP RouteViews


IPv4 BGP
Routing Table
2008-03-01
Announcement Size
/8
/12
/16
/20
/24
/28
/32
Unallocated
HP
DEC
DDN-RVN
GE
Xerox
AT&T
Apple
MIT
DISA
Level3
IANA
Level3
DISA
DISA
ARIN
Unallocated
US Army
IBM
RFC1918
DSI-North
Multicast
Future use
SITA
AT&T
Merit
APNIC
USPS
DoD NIC
Halliburton
PSI
RIPE
ARIN
APNIC
LACNIC
Interop
Eli Lilly
AfriNIC
US-DOD
RIPE
Prudential
Japan Inet
Loopback
LACNIC
Unallocated
Various Registries