"Organisational Structures & Incident Management for Cybersecurity in the Americas"

Dr David E. Probert

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

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

ITU
International
Telecommunication
Union
Committed to connecting the world

Cybersecurity Organisational Structures & Incident Management for CITEL-OAS

1 –Aim: National Cybersecurity	**2 – Critical Service Sectors**	**3 – Cyber Attack Scenarios**
4–"Best Practice" Case Studies	**5–CIRT: Organisational Models**	**6 – The "Cyber" Business Case**
7 – Global IMPACT Alliance	**8 - Public-Private Partnership**	**9 – Next Suggested Steps**

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 • Gaiik • Intel Corporation • Microsoft Corporation • Rossotelecom • Telam • UMTS Forum • VeriSign • Asia Pacific Economic Telecommunication Information Working Group (ApecTel) • African Telecommunication Union (ATU) • Computer Emergency Response Team (CERT) • Commonwealth Telecommunications Organisation (CTO) • Council of Europe • European Network and Information Security Agency (ENISA) • Forum of Incident Response and Security Teams (FIRST) • International Criminal Police Organization (Interpol) • Organisation for Economic Cooperation and Development (OECD) • Organisation internationale de la Francophonie (OIF) • United Nations Institute for Training and Research (UNITAR) • United Nations Office on Drugs and Crime (UNODC) • Carnegie Mellon CyLab (USA) • Ecole Polytechnique Fédérale de Lausanne (EPFL) (Switzerland) • Geneva Security Forum (Switzerland) • Georgia Institute of Technology (USA) • HEC-Université de Lausanne (Switzerland) • Information Security Institute (Australia) • Max-Planck Institute for Foreign and International Criminal Law University (Germany) • Moscow Technical University of Communications (Russian Federation) • Moss Tingrett Court (Norway) • Policyb (Canada) • Queensland University of Technology (Australia) • University of Cologne (Germany).

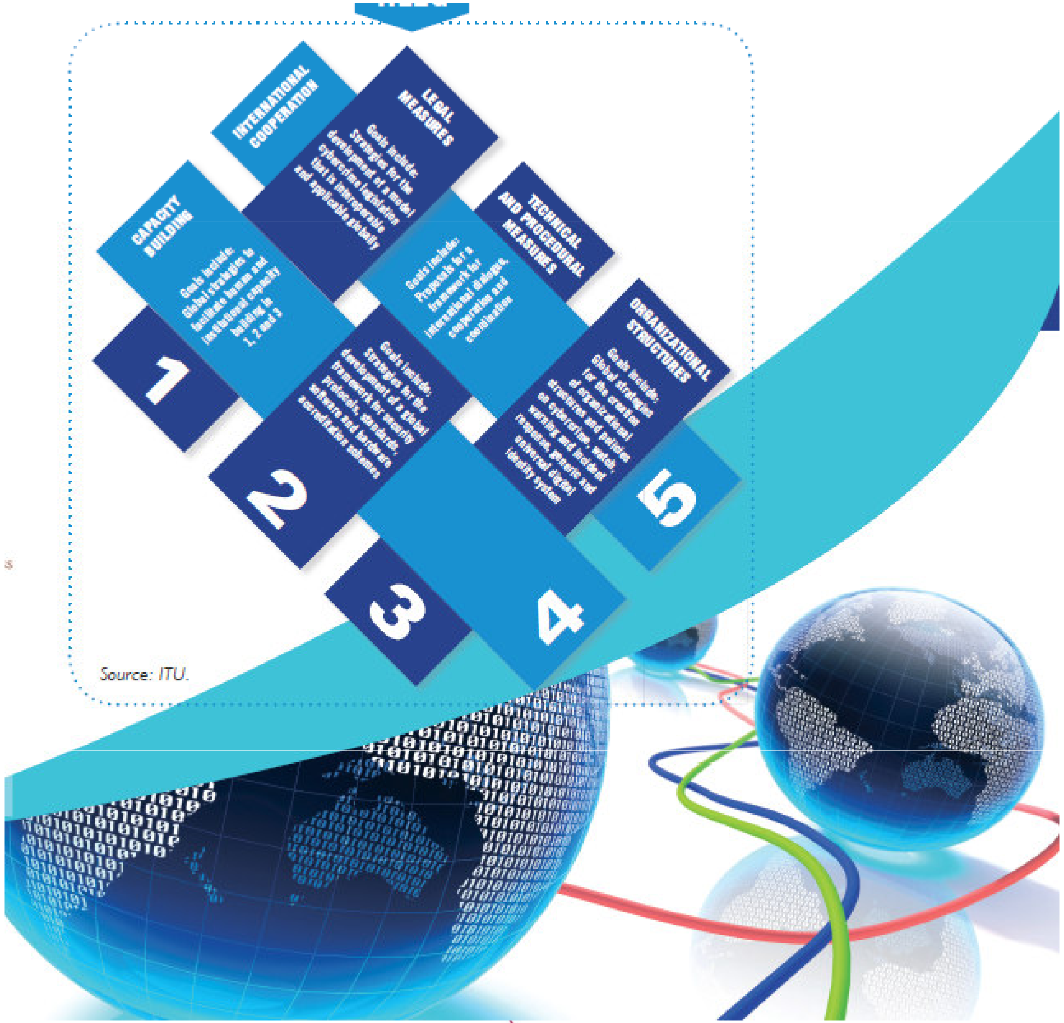
The experts have been invited to join the HLEG because of their world-renowned expertise in the work areas of the GCA and they participate in a personal capacity.

[1] [illegible]

ITU: Committed to connecting the world

International Telecommunication Union

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

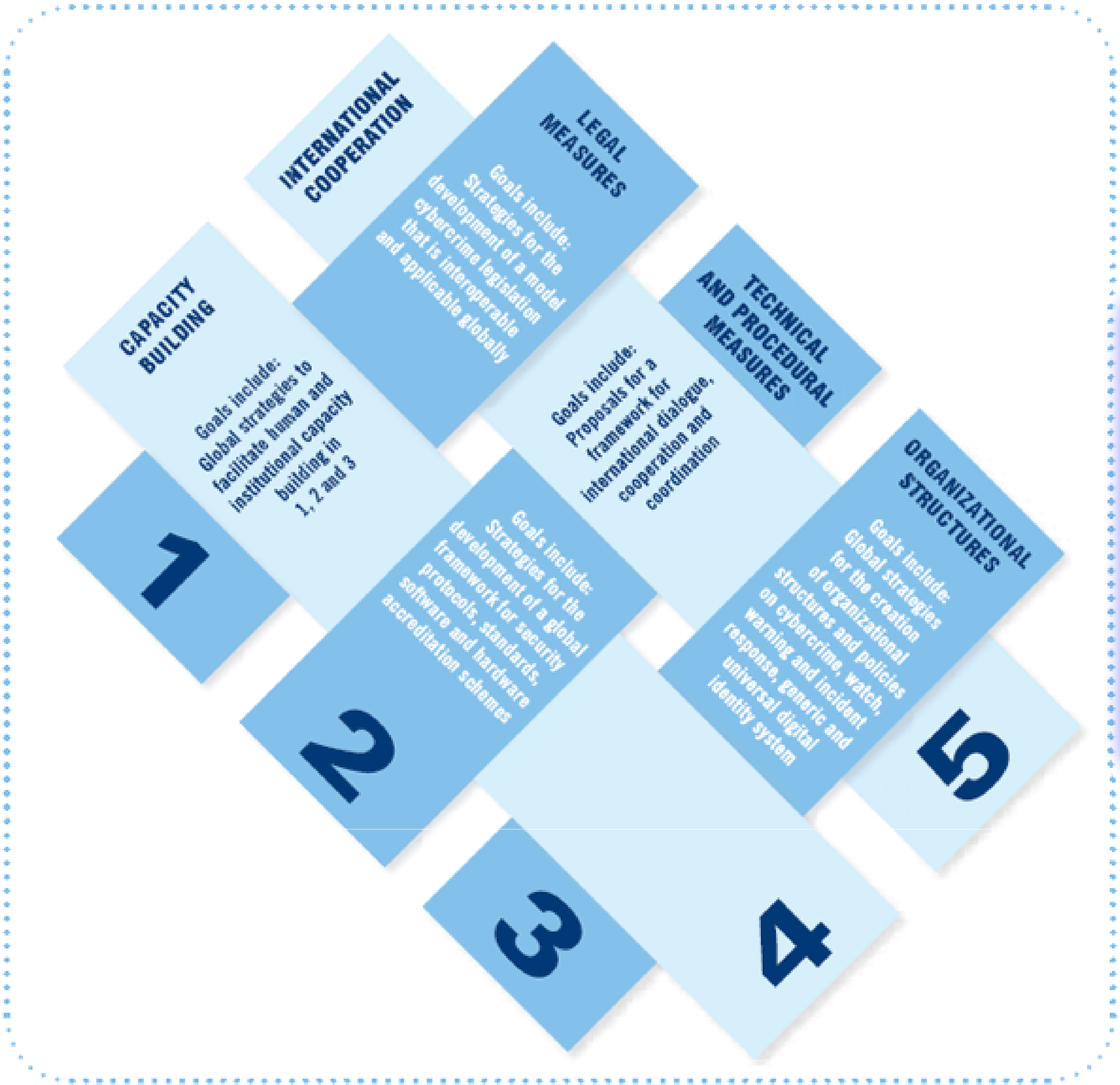


INTERNATIONAL COOPERATION
LEGAL MEASURES
Goals include: Strategies for the development of a model cybercrime legislation that is interoperable and applicable globally
CAPACITY BUILDING
Goals include: Global strategies to facilitate human and institutional capacity building in 1, 2 and 3
TECHNICAL AND 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, and software accreditation schemes
ORGANIZATIONAL STRUCTURES
Goals include: Global strategies for the creation of organizational structures and policies on cybercrime, watch, warning and incident response, and generic and universal digital identity system
1
2
3
4
5

Source: ITU.

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

ITU:– Global Cybersecurity Agenda



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

ORGANIZATIONAL STRUCTURES

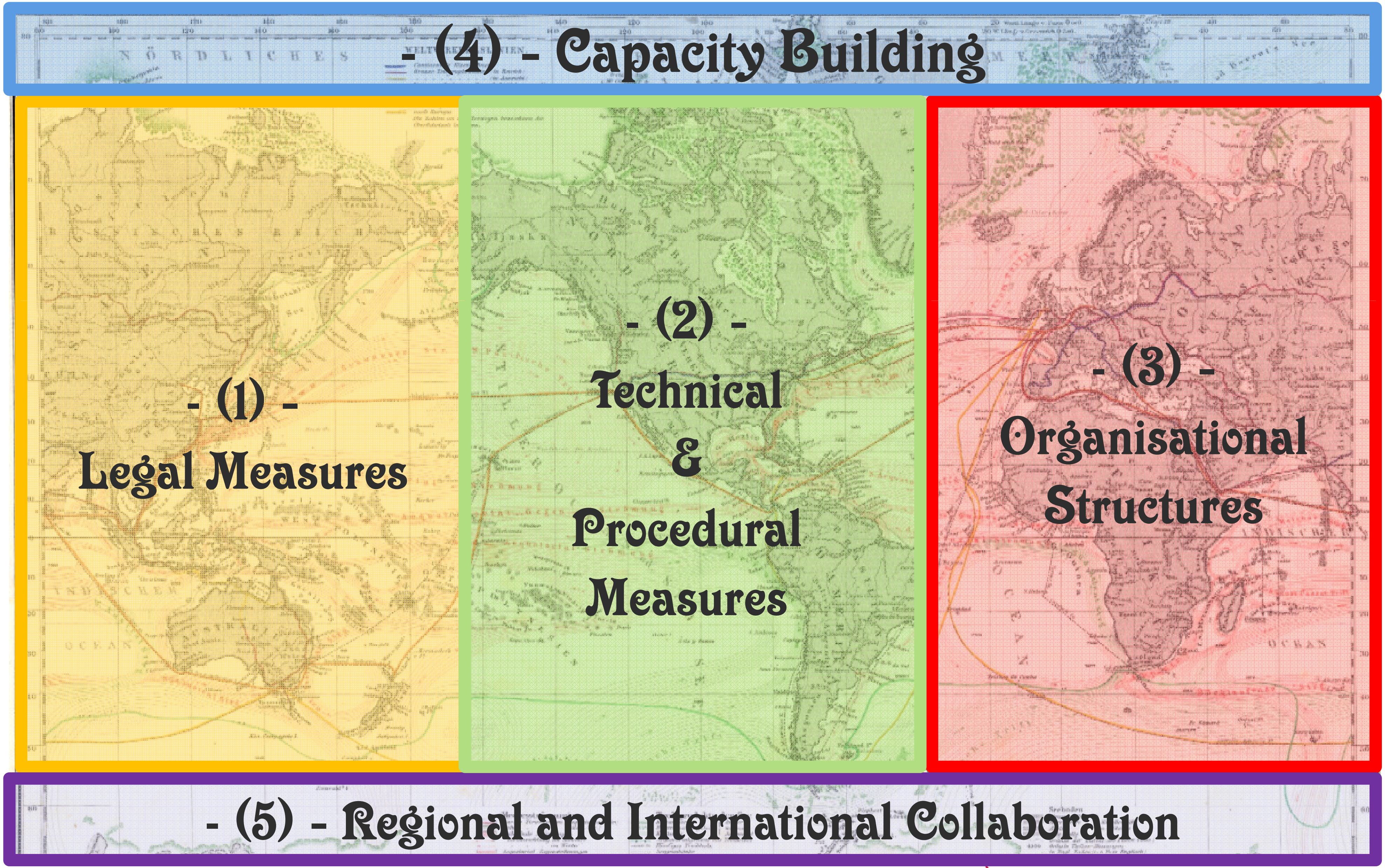
Goals include: Global strategies for the creation of organizational structures and policies on cybercrime, watch, warning and incident response, generic and universal digital identity system

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

The ITU GCA - Global Cybersecurity Agenda:

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

Worldwide Security in Cyberspace!



- (4) - Capacity Building

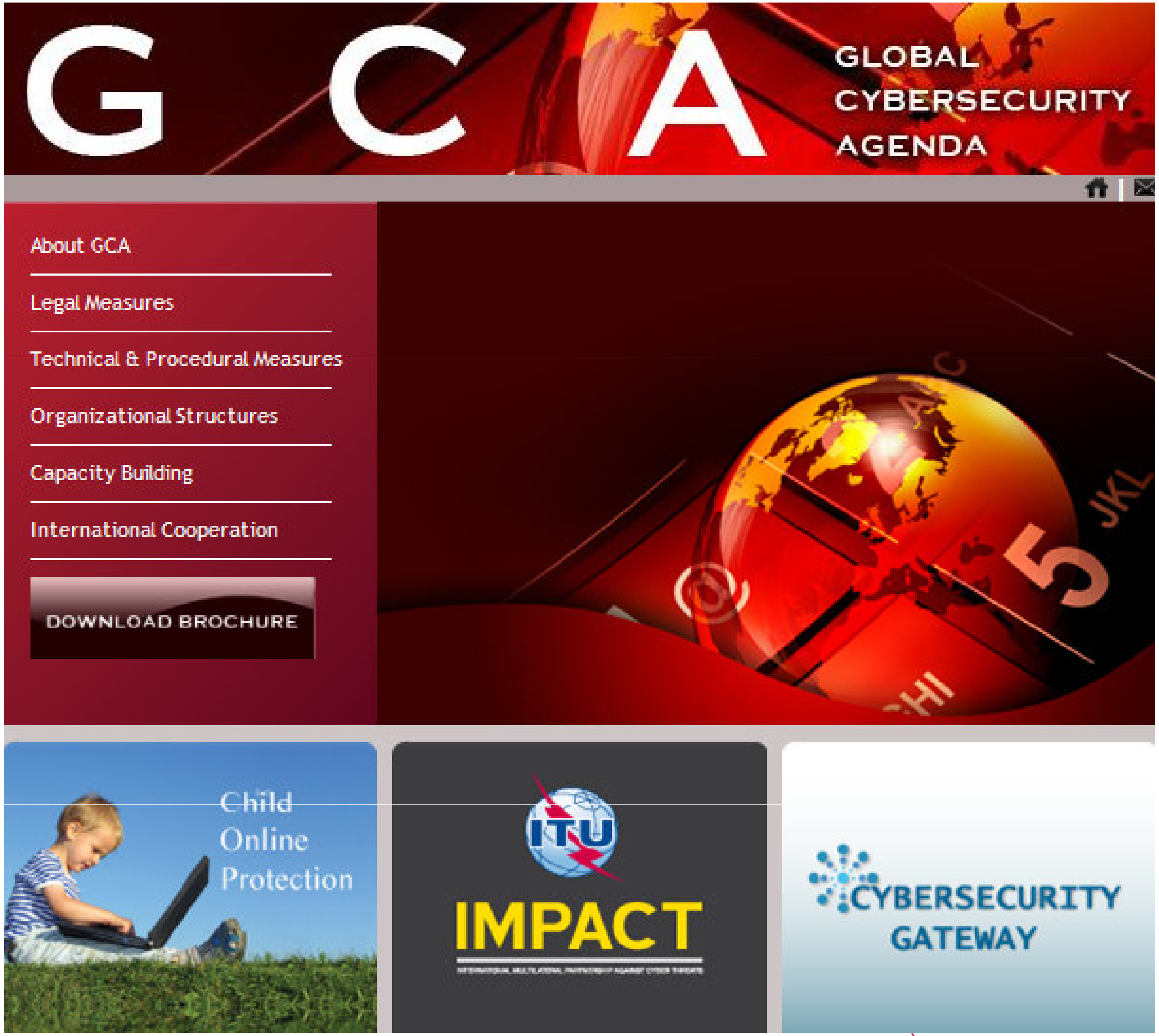
- (1) - Legal Measures

- (2) - Technical & Procedural Measures

- (3) - Organisational Structures

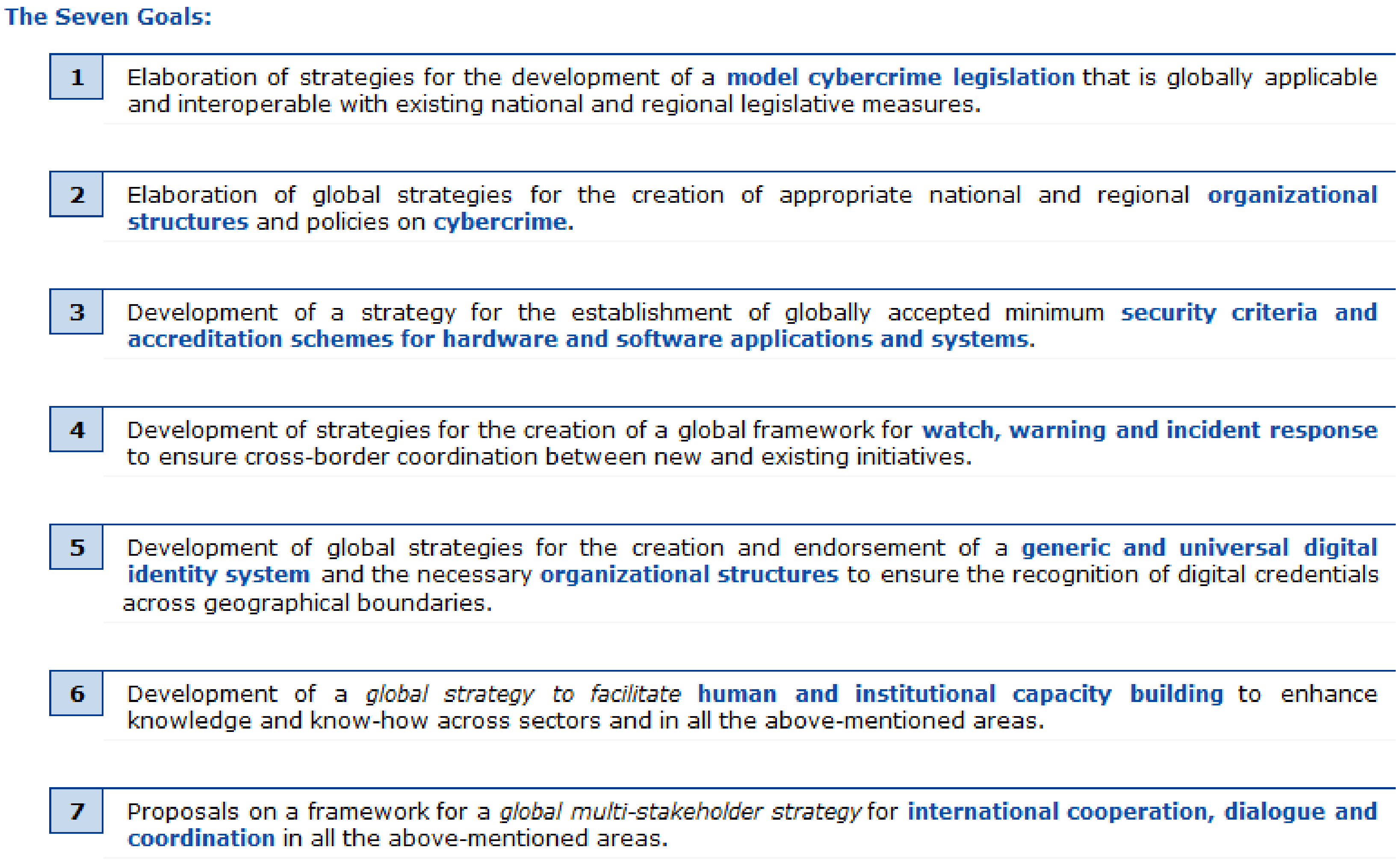
- (5) - Regional and International Collaboration

ITU: Global Cybersecurity Agenda – Web Portal



ITU GCA – The Seven Strategic Goals

- for National & International Cybersecurity -



The Seven Goals:

1 Elaboration of strategies for the development of a **model cybercrime legislation** that is globally applicable and interoperable with existing national and regional legislative measures.

2 Elaboration of global strategies for the creation of appropriate national and regional **organizational structures** and policies on **cybercrime.**

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

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

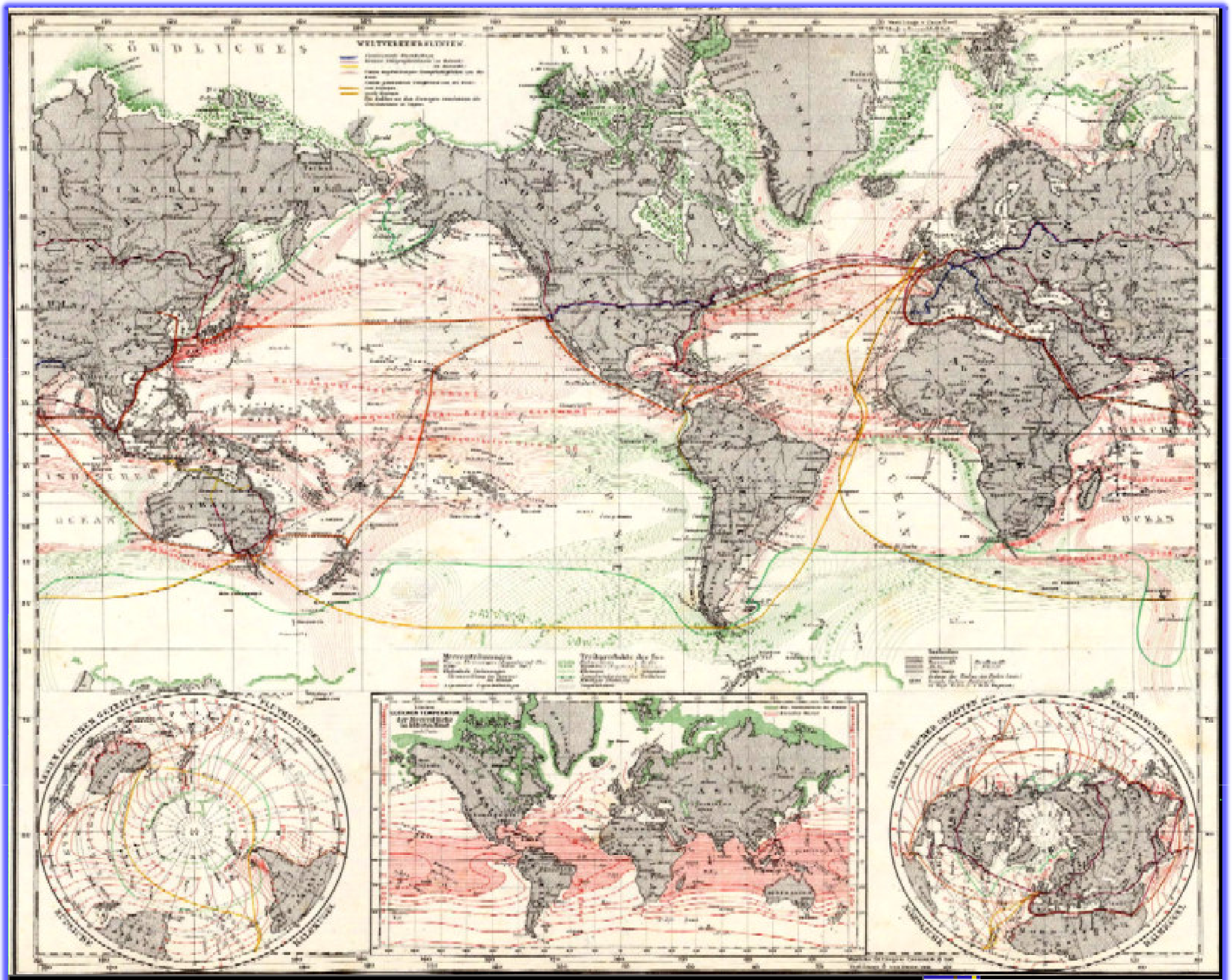
5 Development of global strategies for the creation and endorsement of a **generic and universal digital identity system** and the necessary **organizational structures** to ensure the recognition of digital credentials across geographical boundaries.

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

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

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

“Visualisation of Cyberspace”: Global IP “WHOIS” Addresses



…From 20thC Physical World To 21stC Cyberspace! ...

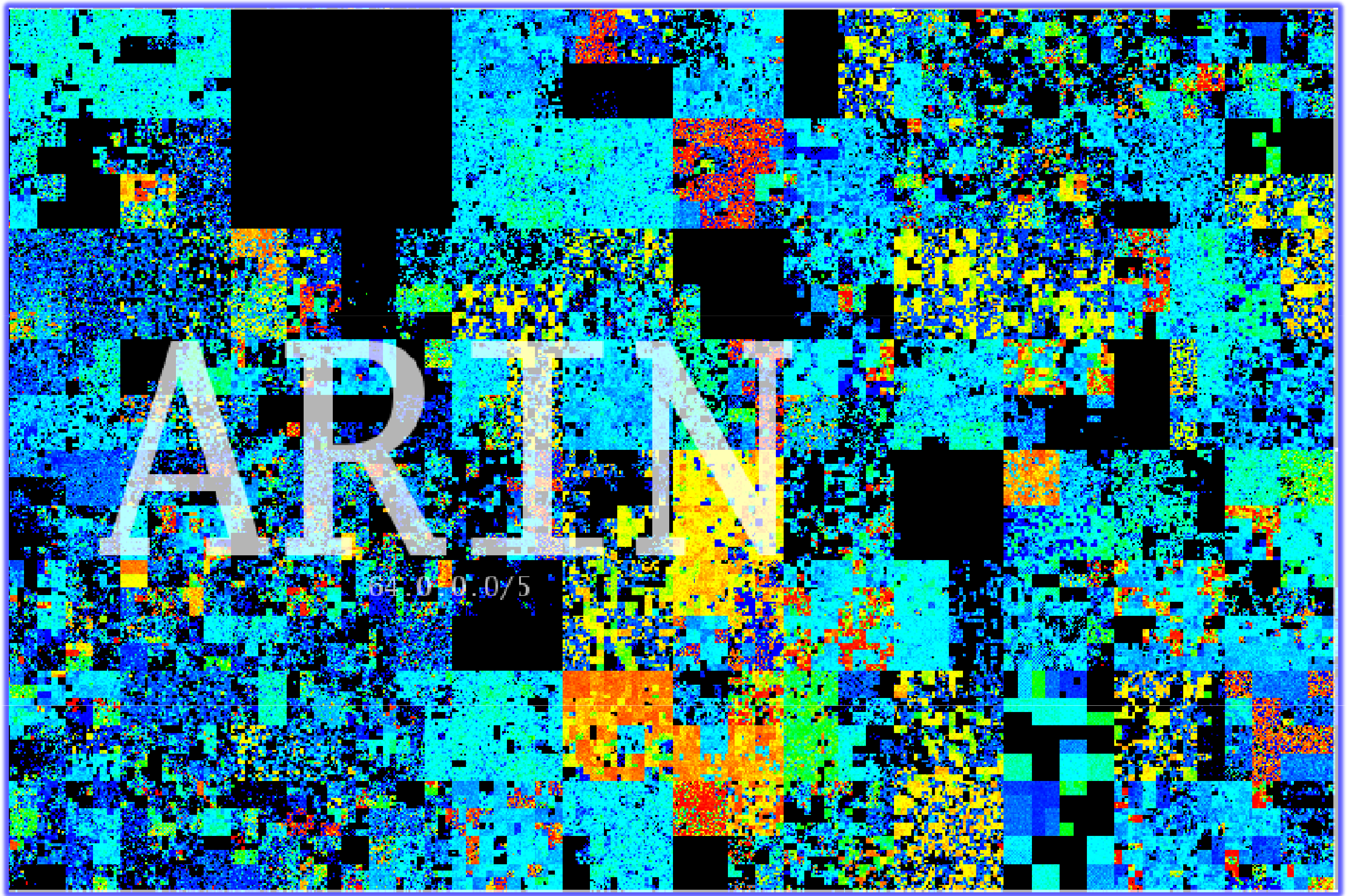
Organización de los Estados Americanos
Organização dos Estados Americanos
Organisation des États Américains
Organization of American States

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

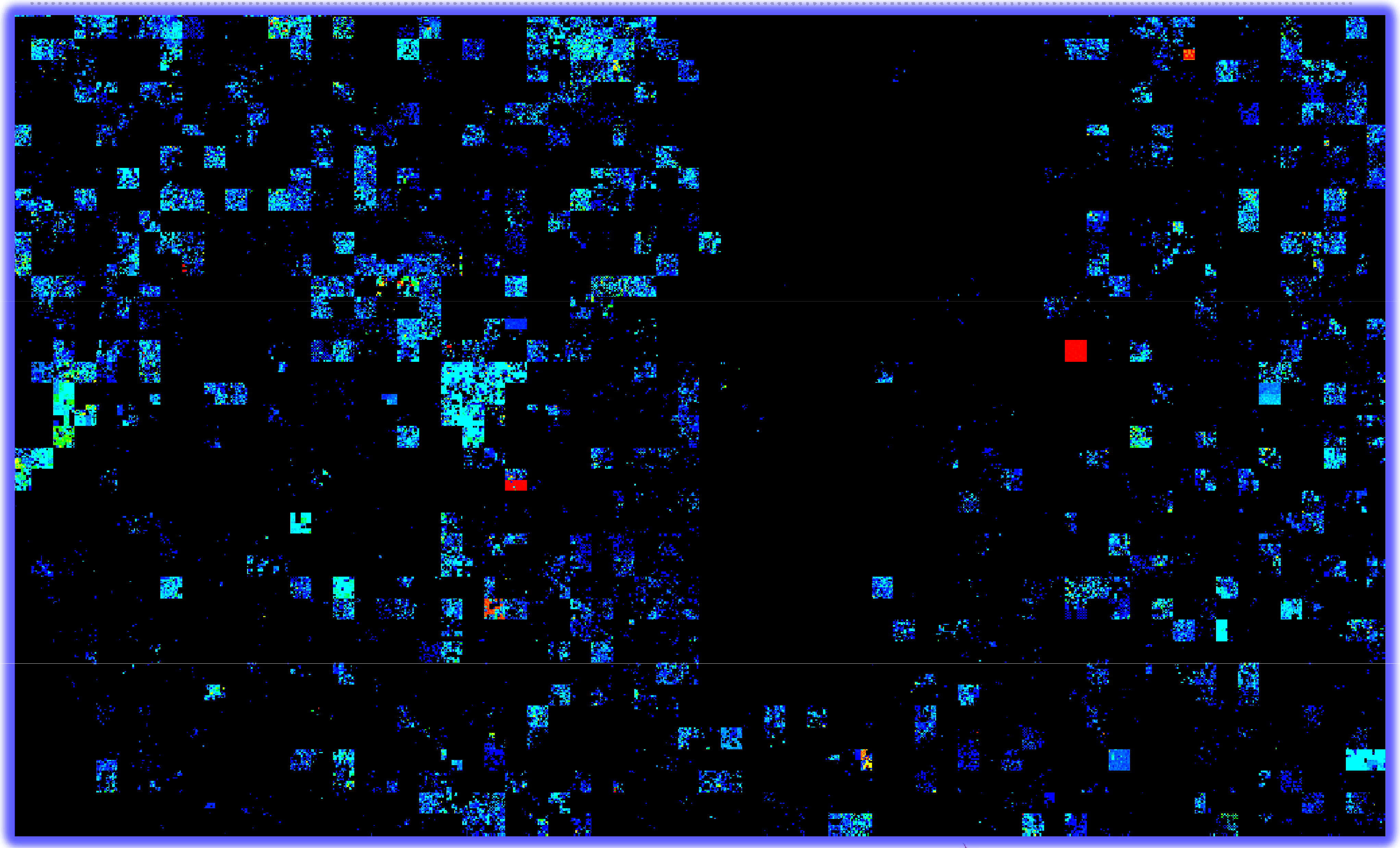
International
Telecommunication
Union

Committed to connecting the world

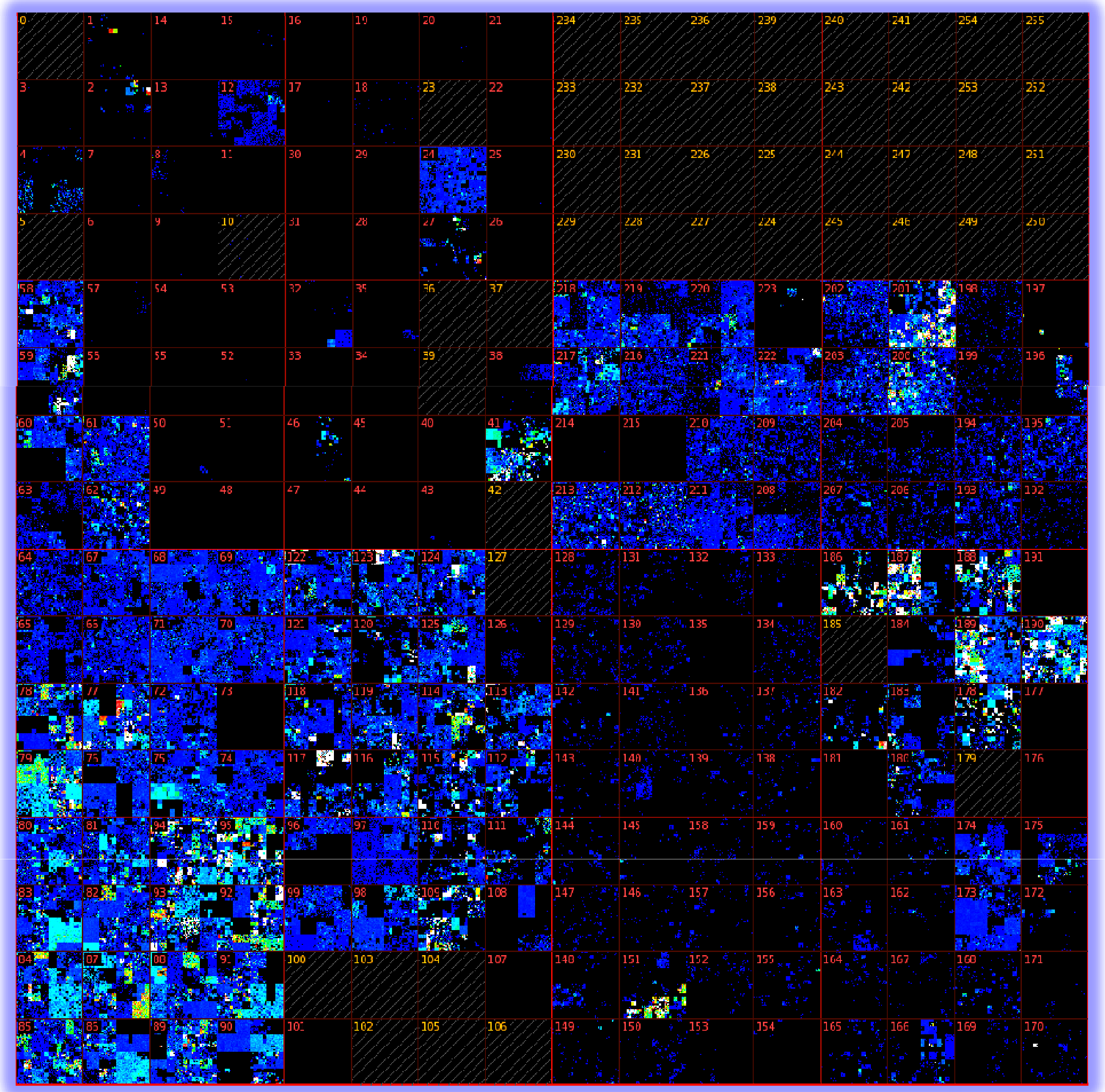
Active Internet Domains – "American IP Registry"



“Outer Galaxies of Cyberspace” – Other Registries



Malicious Cybercrime Activity in Global Cyberspace



Key: Hilbert Space-Filling Curve Process

Link: www.team-cymru.org

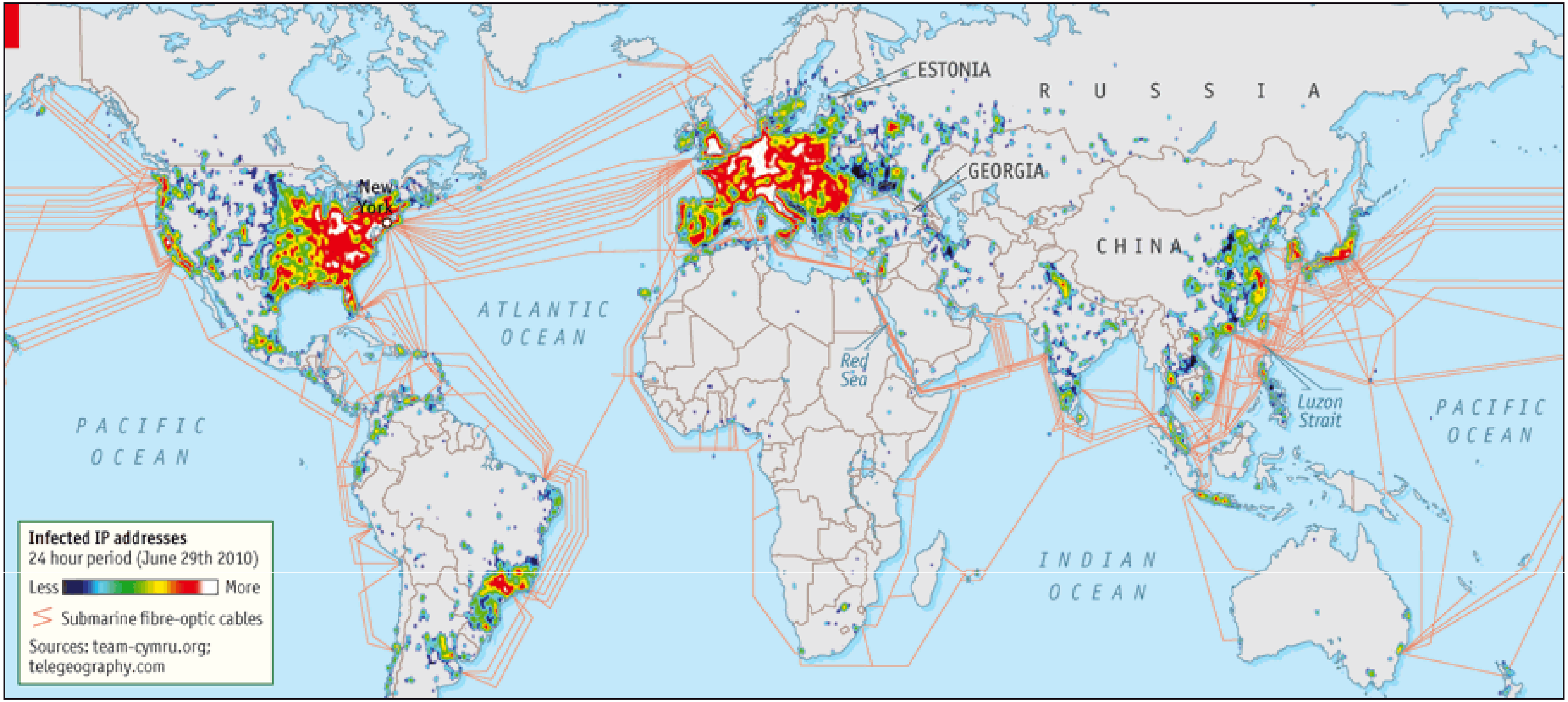
Organización de los Estados Americanos
Organização dos Estados Americanos
Organisation des États Américains
Organization of American States

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

International Telecommunication Union

Committed to connecting the world

Global IP Connectivity: *Real-Time Infection*



Sources: team-cymru.org; telegeography.com

Implementation of ITU's GCA Framework

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

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

Cybersecurity Organisational Structures & Incident Management for CITEL-OAS

1 –Aim: National Cybersecurity	2 – Critical Service Sectors	3 – Cyber Attack Scenarios
4–"Best Practice" Case Studies	5–CIRT: Organisational Models	6 – The "Cyber" Business Case
7 – Global IMPACT Alliance	8 - Public-Private Partnership	9 – Next Suggested Steps

Critical Service Sector Infrastructure

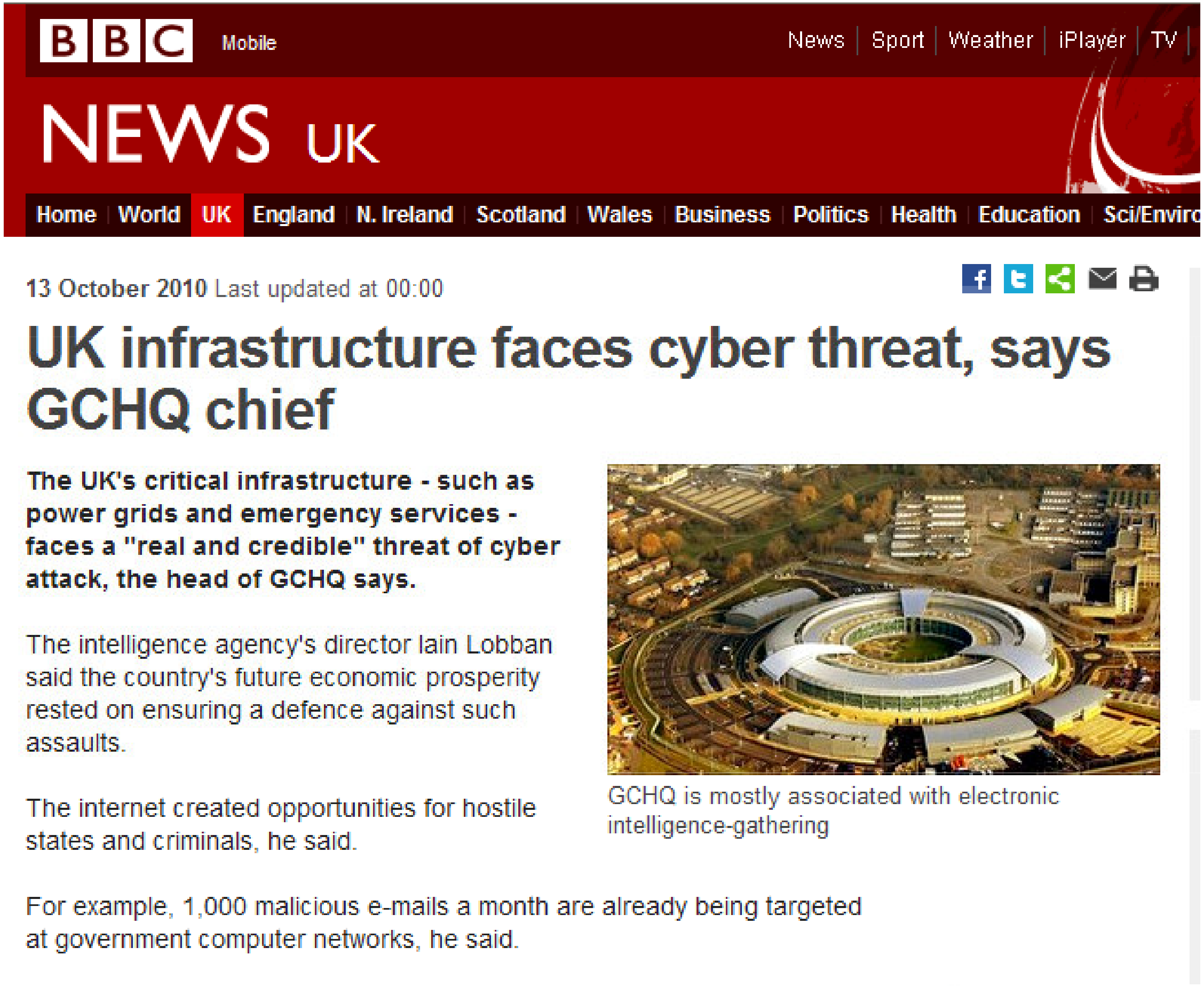
- National Strategies: Many countries now consider the threat of cyber attacks to be high enough to establish national cybersecurity strategies.

- UK Strategy: As with physical security & defence, these should be annually updated. For example the UK published its 1st Cybersecurity Strategy (June 2009), and now an updated UK National Security Strategy (Oct 2010).

- Every Critical Service Sector should be strategically addressed in-depth:
  - Government (National & Regional)
  - Telecomms/Mobile/ISPs
  - Banking/Financial Services
  - Transportation/Airports/Ports
  - Energy Power Grid & Utilities
  - Healthcare & Emergency Services
  - Police & Law Enforcement Agencies

….The national cybersecurity organisation will include all these sector stakeholders, whilst the CIRTs will respond to incidents & communicate cyber alerts & emergency actions across ALL sectors

Cyber Threats against UK Critical Services


BBC
Mobile
News | Sport | Weather | iPlayer | TV
NEWS UK
Home | World | UK | England | N. Ireland | Scotland | Wales | Business | Politics | Health | Education | Sci/Enviro

13 October 2010 Last updated at 00:00

UK infrastructure faces cyber threat, says GCHQ chief

The UK's critical infrastructure - such as power grids and emergency services - faces a "real and credible" threat of cyber attack, the head of GCHQ says.

The intelligence agency's director Iain Lobban said the country's future economic prosperity rested on ensuring a defence against such assaults.

The internet created opportunities for hostile states and criminals, he said.

GCHQ is mostly associated with electronic intelligence-gathering

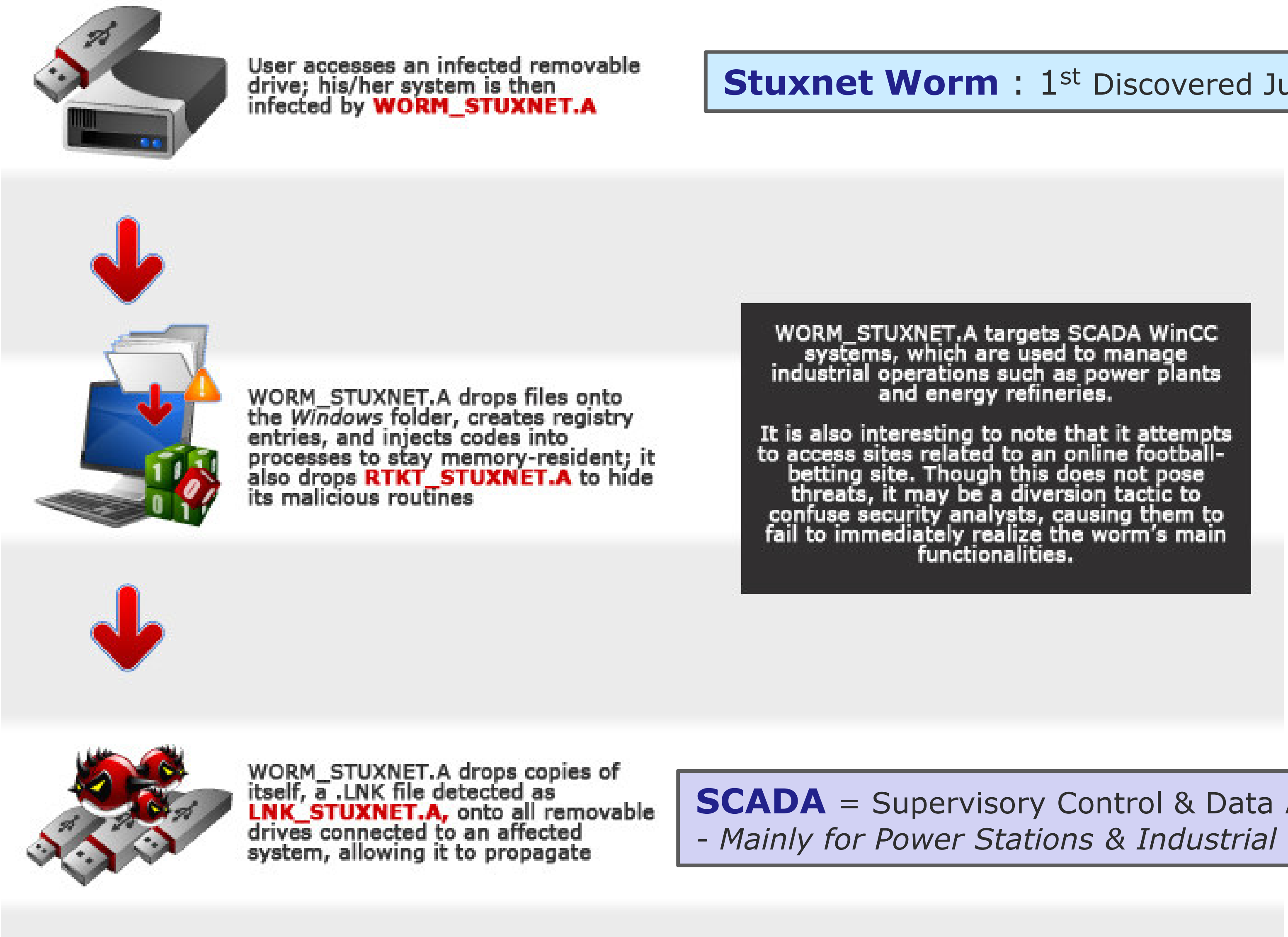
For example, 1,000 malicious e-mails a month are already being targeted at government computer networks, he said.

CyberCrimes against Critical Sectors

- *Government:*
  - Theft of secret intelligence, manipulation of documents, and illegal access to confidential citizen databases & national records
- *Banking/Finance:*
  - Denial of Service attacks against clearing bank network, phishing attacks against bank account & credit cards, money laundering
- *Telecomms/Mobile:*
  - Interception of wired & wireless communications, and penetration of secure government & military communications networks
- *Transport/Tourism:*
  - Cyber Terrorism against airports, air-traffic control, coach/train transport hubs, & malicious penetration of on-line travel networks
- *Energy/Water:*
  - Manipulation and disruption of the national energy grid & utilities through interference of the process control network (SCADA)

Case Study: StuxNet Worm - Industrial SCADA Systems

Stuxnet Worm : 1st Discovered June 2010



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

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

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

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

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

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

Cybersecurity Organisational Structures & Incident Management for CITEL-OAS

1 –Aim: National Cybersecurity	2 – Critical Service Sectors	3 – Cyber Attack Scenarios
4–"Best Practice" Case Studies	5–CIRT: Organisational Models	6 – The "Cyber" Business Case
7 – Global IMPACT Alliance	8 - Public-Private Partnership	9 – Next Suggested Steps

Sources of Cyber Threats

- The complexity of cyber threats means that several complimentary frameworks have been developed that classify the risks:
- For this workshop session we'll focus on the categorisation developed by the *ITU Telecommunications Study Group 17* as follows:

Category 1 : Unauthorised Access *– The systems & networks are accessed by persons or "bots" that do not have legal access or permissions*

Category 2 : Denial of Service Attacks (DoS) *– Such attacks are used to target & disable a specific website or server using an army of infected machines*

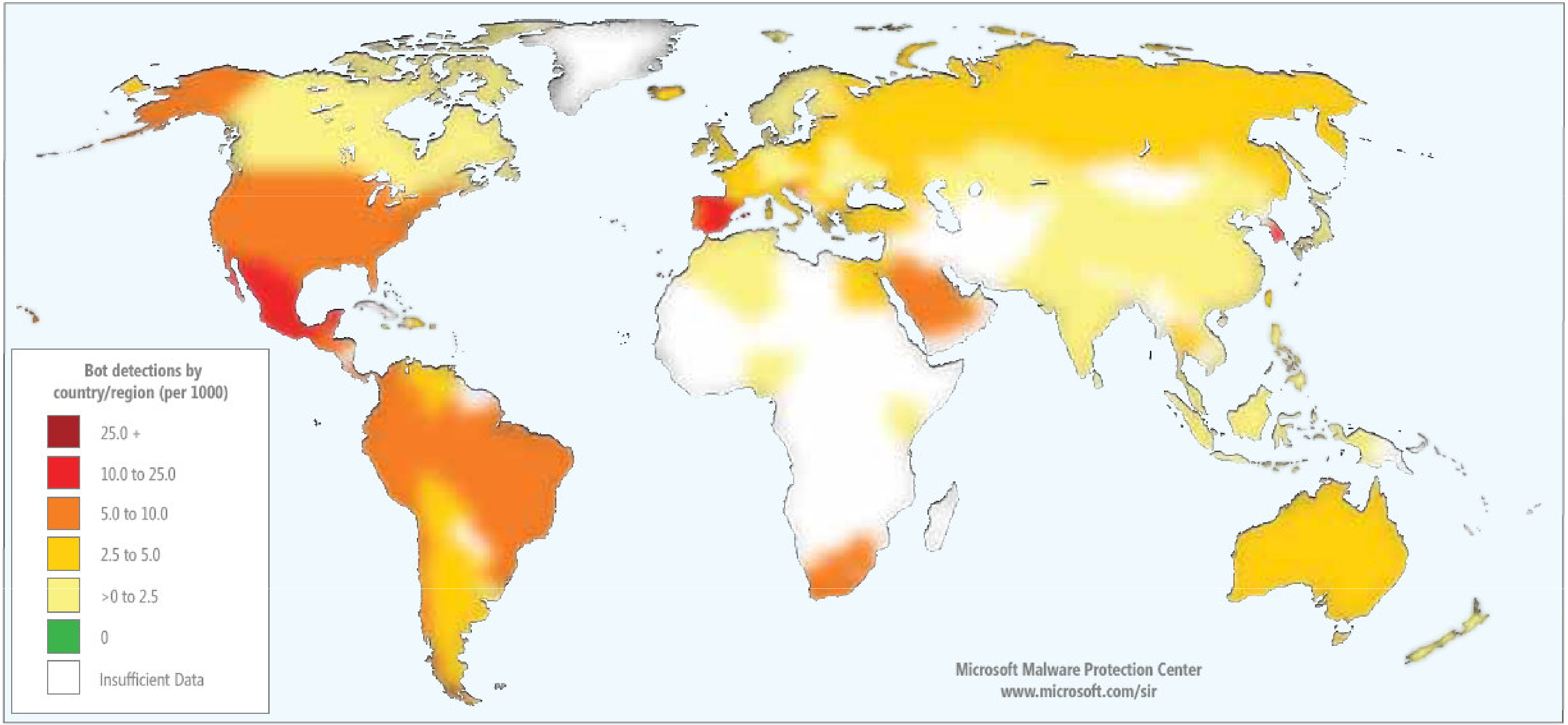
Category 3 : Malicious Code *– Malware such as trojans, viruses & spyware are embedded within host machines for both commercial & criminal purposes*

Category 4 : Improper Use of Systems *– In these cases, the systems are being used for access and applications against the communicated policies*

Category 5 : Unauthorised Access AND Exploitation *– Many attacks will fall into this category when the hacker will penetrate systems and then use the acquired data, information & documents for cybercriminal activities*

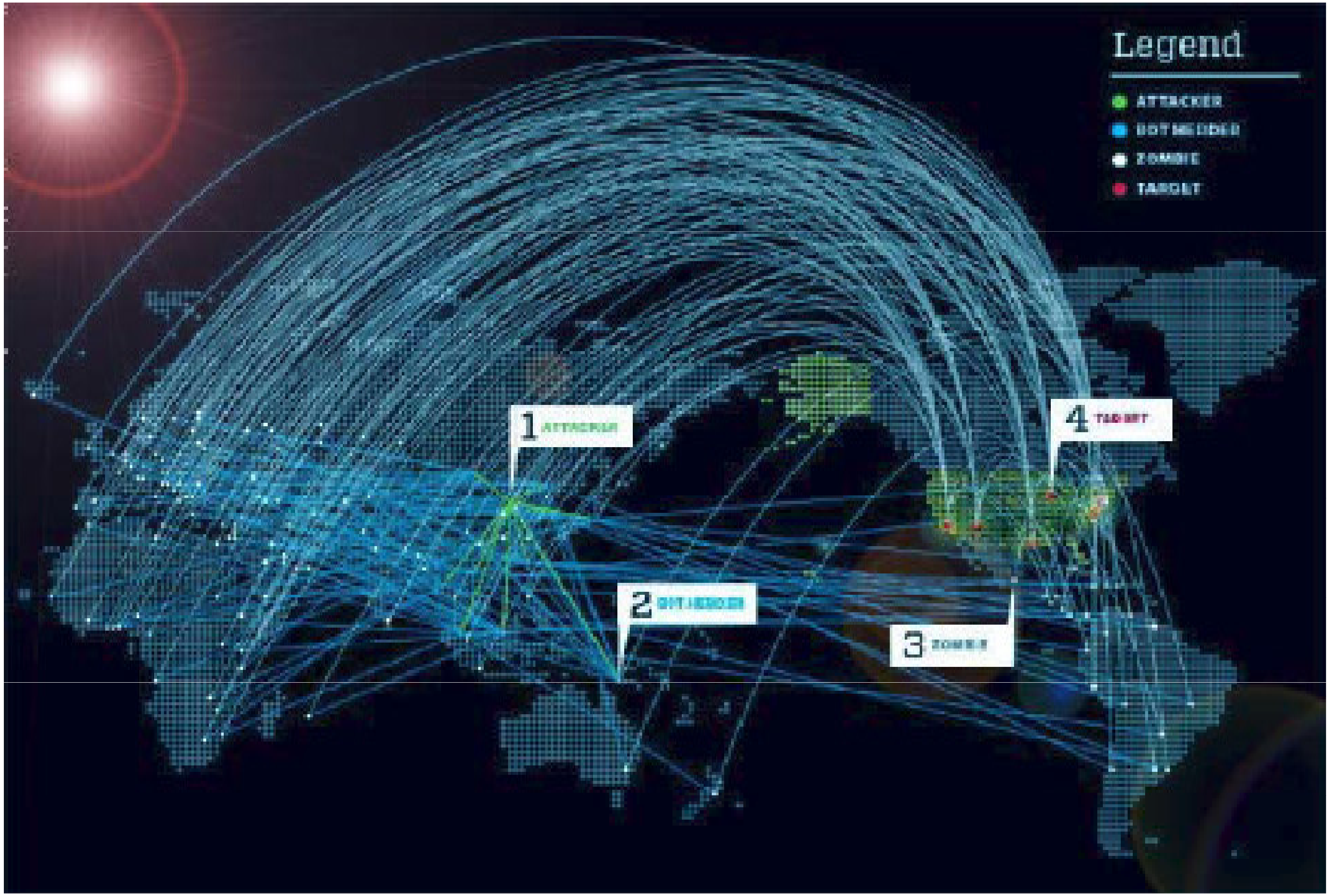
Category 6 : Other Unconfirmed Incidents *– These are alerts that require further investigation to understand whether they are actually malicious*

Regional "Bot" Infections – 2Q 2010



Source: Microsoft – Security Intelligence Report - 2010

Typical "Botnet" Cyberattack



Cyber Attacks: Criminal Industrialisation

- Industrialisation and Mainstreaming of Cyber Attacks:
  - *(1) Researchers & Cyber Software Creators of Malicious Codes* : Often creative talented computer scientists that have turned their skills to tools for illegal penetration & control of secure systems
  - *(2) "Botnet" - Farmers & Herders* : They are responsible for the illegal international distribution and infection of target "zombie" networked laptops PCs & Servers within homes and offices. The malicious codes (malware such as viruses & trojans) are spread through spam emails, infected websites and "backdoor" attacks.
  - *(3) "Commercial Botnet Dealers"* : They sell access to herds of "zombie" infected machines. The embedded malicious code can be triggered to stimulate "Denial of Service (DDoS)" attacks on target servers & websites. The aim is usually to maximise economic and political damage upon the targeted nation and associated businesses.

...For further information: ITU "BotNet" Mitigation Toolkit

Recent Cyber Attacks: Case Studies

- *Estonia : May 2007*
  - Targeted at Government & Banking Servers – and immobilised national & commercial economic infrastructure for several days
- *Georgia : August 2008*
  - Targeted at Government Servers including Parliament & Ministry of Foreign Affairs, and the National & Commercial Banking Network.
- *South Korea : July 2009*
  - Targets included the Defence Ministry, Presidential Offices, National Assembly, and Korea Exchange Banks. This attack was also simultaneously targeted at various high-profile US Sites & Servers such as the NY Stock Exchange, White House & Pentagon.

…….Small scale penetrations & cyber attacks continue on an almost 24/7 against certain countries, targeted regimes and business interests.

Cybersecurity Organisational Structures & Incident Management for CITEL-OAS

1 –Aim: National Cybersecurity	2 – Critical Service Sectors	3 – Cyber Attack Scenarios
4–“Best Practice” Case Studies	5–CIRT: Organisational Models	6 – The “Cyber” Business Case
7 – Global IMPACT Alliance	8 - Public-Private Partnership	9 – Next Suggested Steps

National Cybersecurity Agency: Case Studies

- *US Government:* Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure – May 2009
- *Canada:* Canadian Cyber Incident Response Centre (CCIRC) – Integrated within the Strategic Government Operations Centre (GOC)
- *UK Government:* Cybersecurity Strategy for the UK – Safety, Security & Resilience in Cyberspace (UK Office of Cybersecurity – June 2009)
- *Australia:* Australian Cybersecurity Policy and Co-ordination Committee (CSPC – Nov 2009), within the Attorney-General's Government Dept
- *Malaysia:* "Cybersecurity Malaysia" – Mosti : Ministry of Science, Technology & Innovation, and includes the MyCERT & Training Centre
- *Singapore:* Cybersecurity Awareness Alliance & the IDA Security Masterplan (Sept 2009) -Singapore Infocomm Techology Security Authority - SITSA
- *South Korea:* Korea Internet and Security Agency (KISA – July 2009)

…..Many nations are now also following similar strategies and using their National CIRTs as the focus & catalyst to develop national cyber agencies

US Government : Office of CyberSecurity (CS&C)

- Following the June 2009, US Government Policy Review, the Department of Homeland Security (DHS) has responsibility for hosting the *"Office of Cybersecurity and Communications" (CS&C)*. Within this large organisation is the "*National Cyber Security Division" (NCSD):*
  - *National Cyberspace Response System*
    - National Cyber Alert System
    - US-CERT Operations
    - National Cyber Response Co-ordination Group
    - Cyber Cop Portal (for investigation and prosecution of cyber attacks)
  - *Federal Network Security*
    - Ensuring the maximum security of executive civilian departments and agencies
  - *Cyber-Risk Management Programs*
    - Cyber Exercises: Cyber Storm
    - National Outreach Awareness
    - Software Assurance Program

….The US Government DHS also has a National Cyber Security Center (NCSC) which is tasked with the protection of the US Government's Communications Networks

Canadian Government

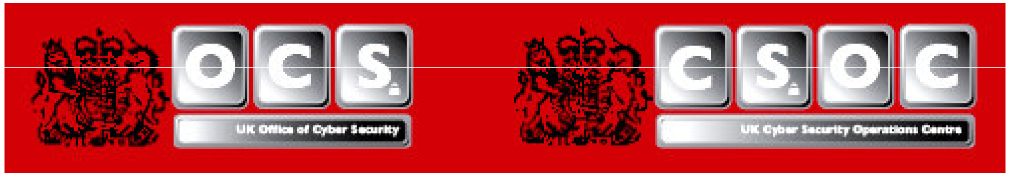
- The Canadian Cyber Incident Response Centre (CCIRC) monitors the cyber threat environment around the clock and is responsible for coordinating the national response to any cyber security incident. Its focus is the protection of national critical infrastructure against cyber incidents. The Centre is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

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

UK Office of Cybersecurity – OCS & CSOC

Cyber Security Strategy of the United Kingdom

safety, security and resilience in cyber space


OCS
UK Office of Cyber Security
CSOC
UK Cyber Security Operations Centre

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

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

Australian Government : CSPC

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

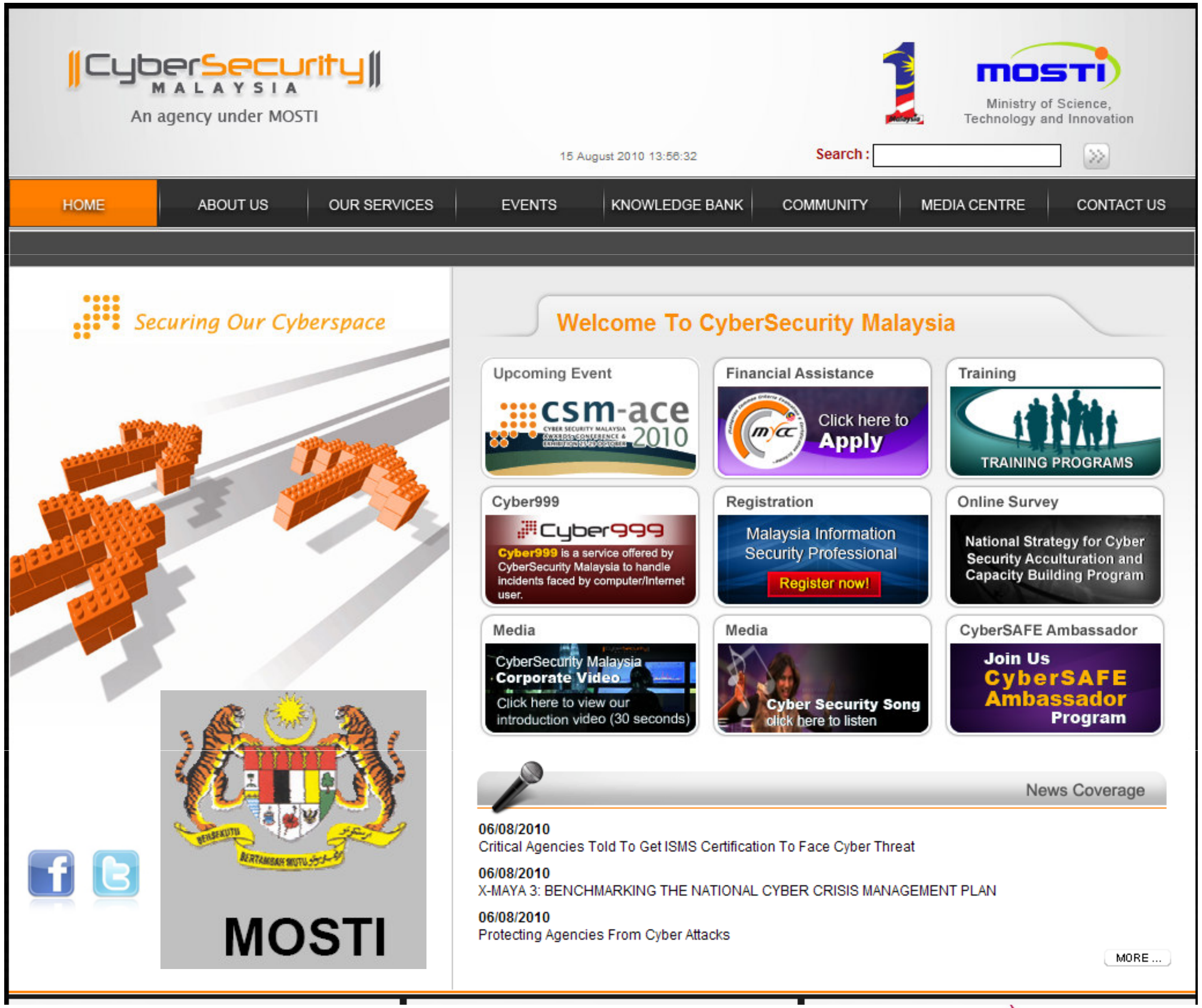
Cyber Security Operations Centre (CSOC)

Australian Government

CERT Australia

AUSTRALIA'S NATIONAL
COMPUTER EMERGENCY RESPONSE TEAM

Malaysian Government: MOSTi



Welcome To CyberSecurity Malaysia

Upcoming Event: csm-ace 2010, Cyber Security Malaysia Awards, Conference & Exhibition 25-29 October

Financial Assistance: Click here to Apply

Training: TRAINING PROGRAMS

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

Registration: Malaysia Information Security Professional. Register now!

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

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

Media: Cyber Security Song. click here to listen

CyberSAFE Ambassador: Join Us CyberSAFE Ambassador Program

News Coverage

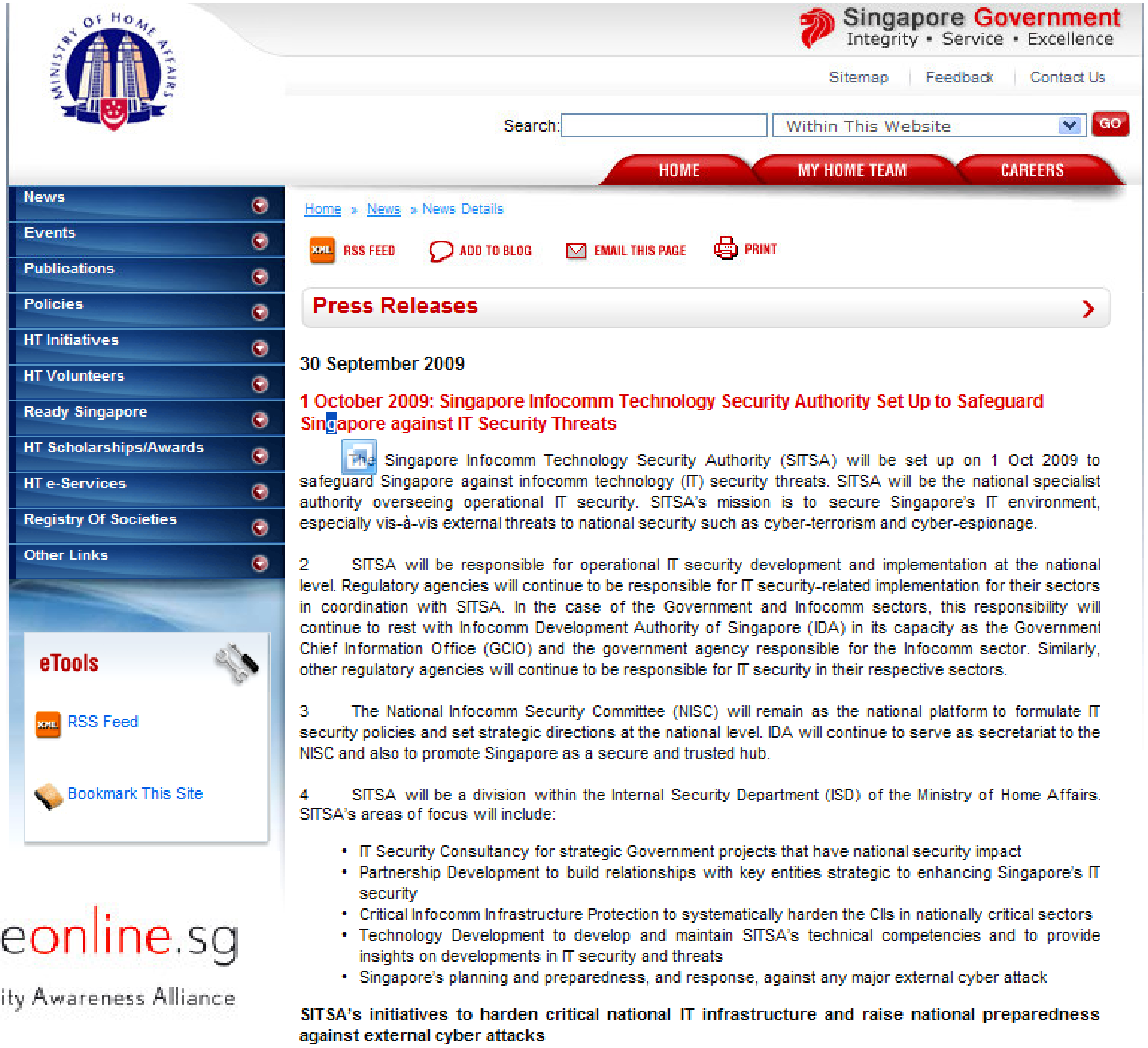
06/08/2010
Critical Agencies Told To Get ISMS Certification To Face Cyber Threat

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

06/08/2010
Protecting Agencies From Cyber Attacks

MORE ...

Singapore Government : SITSA



Press Releases

30 September 2009

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

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

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

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

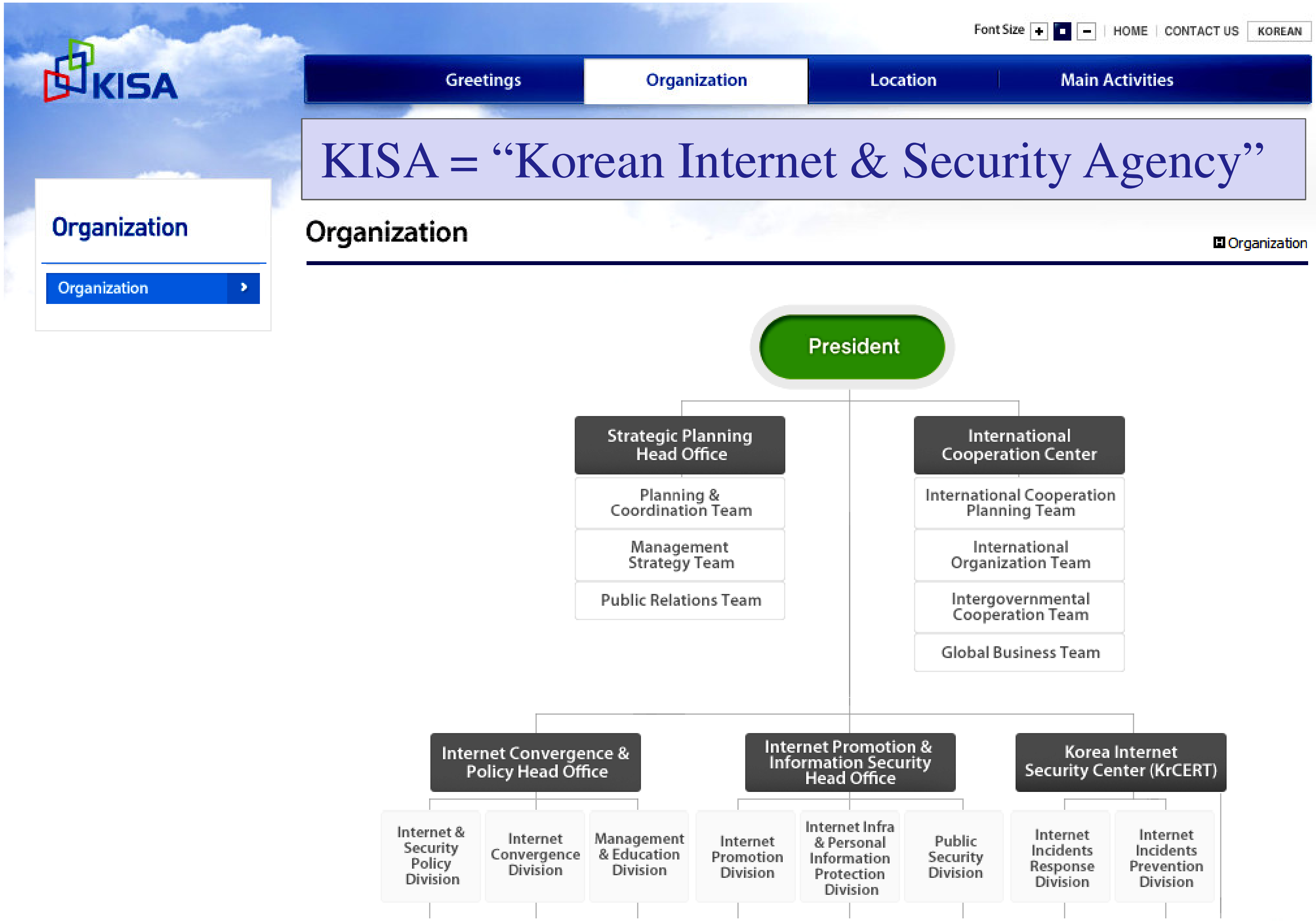
4 SITSA will be a division within the Internal Security Department (ISD) of the Ministry of Home Affairs. SITSA's areas of focus will include:

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

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

GOsafeonline.sg
Cyber Security Awareness Alliance

South Korea Government: KISA



Font Size + ■ − | HOME | CONTACT US | KOREAN

KISA

Greetings | Organization | Location | Main Activities

KISA = “Korean Internet & Security Agency”

Organization

Organization ›

Organization

■ Organization

President

- Strategic Planning Head Office
  - Planning & Coordination Team
  - Management Strategy Team
  - Public Relations Team
- International Cooperation Center
  - International Cooperation Planning Team
  - International Organization Team
  - Intergovernmental Cooperation Team
  - Global Business Team
- Internet Convergence & Policy Head Office
  - Internet & Security Policy Division
  - Internet Convergence Division
  - Management & Education Division
- Internet Promotion & Information Security Head Office
  - Internet Promotion Division
  - Internet Infra & Personal Information Protection Division
  - Public Security Division
- Korea Internet Security Center (KrCERT)
  - Internet Incidents Response Division
  - Internet Incidents Prevention Division

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

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

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

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

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

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

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

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

National Cybersecurity Agencies: Common Roles

- Common roles and responsibilities for all these national cyber agencies:
  - *Cyber Alerts:* Management of the National Response to Cyber Alerts, and Attacks
  - *Education:* Co-ordination of the National Awareness and Skills Training Programmes
  - *Laws:* Leadership role in the development and approval of new cyber legislation
  - *Cybercrime:* Facilitation for building a National Cybercrime of e-Crime Unit
  - *Standards:* Setting the national cybersecurity standards and auditing compliance
  - *International:* Leadership in the promotion of international partnerships for
  - *Research:* Support for research & development into cybersecurity technologies
  - *Critical Sectors:* Co-ordination of National Programmes for Critical Infrastructure

...Next we consider the ITU's standards based approach to the organisation of a national or critical sector Computer Incident Response Team (CIRT)…

Cybersecurity Organisational Structures & Incident Management for CITEL-OAS

1 –Aim: National Cybersecurity	2 – Critical Service Sectors	3 – Cyber Attack Scenarios
4–"Best Practice" Case Studies	5–CIRT: Organisational Models	6 – The "Cyber" Business Case
7 – Global IMPACT Alliance	8 - Public-Private Partnership	9 – Next Suggested Steps

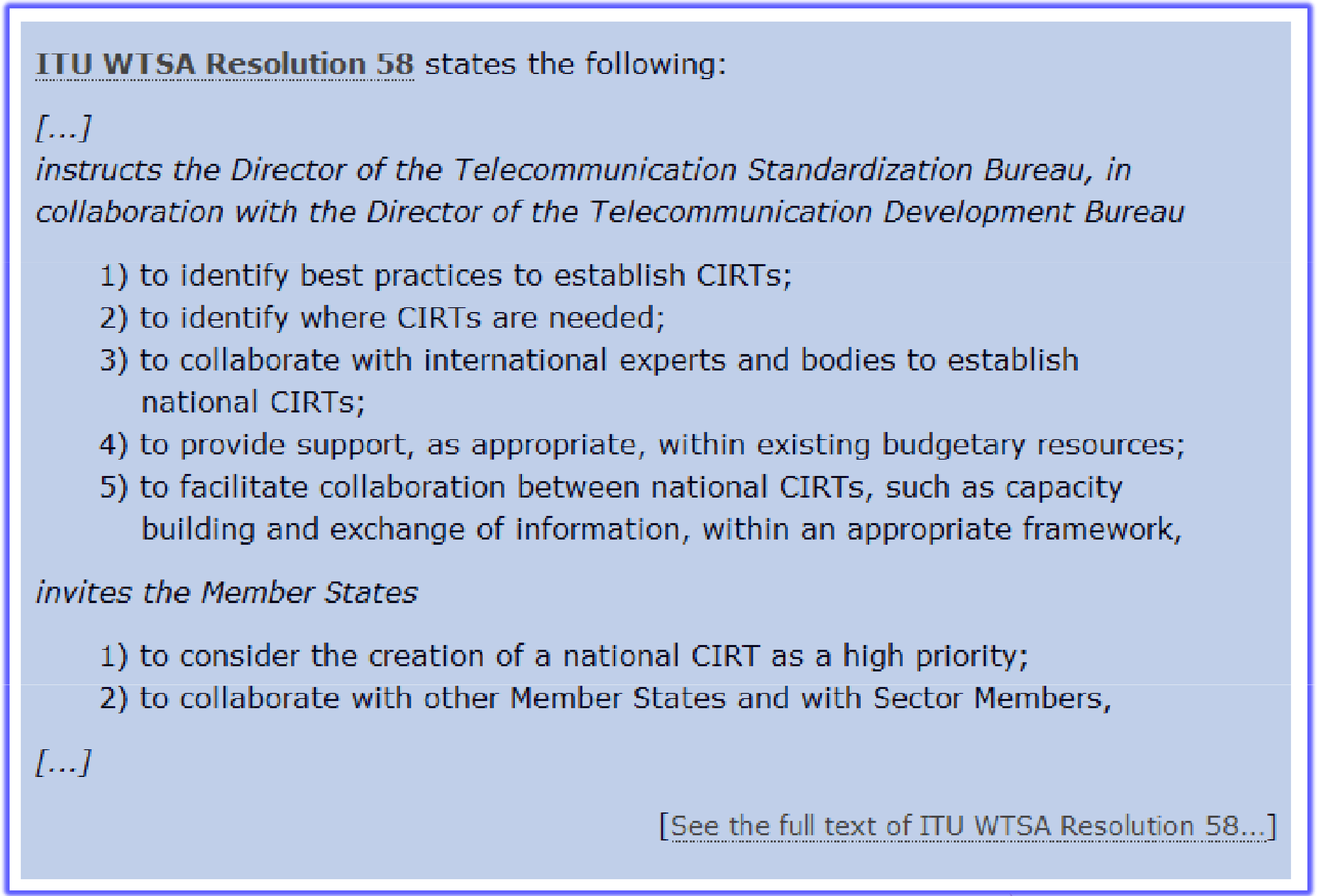
ITU's Strategic Vision on National CIRTs – Organisation & Benefits

- ITU sees *major* national strategic & operational benefits from CIRTs which may provide strong national foundations and catalysts for:

1) Human Capacity Building
2) Cybercrime Legislation & Training
3) eGovernment Framework & Applications
4) Child On-Line Protection Programme
5) National Identity & Access Management
6) Cybersecurity Culture & Awareness Programme
7) Enhanced Incident Response & Management
8) Cyber Event Prevention & Mitigation Strategy
9) Disaster & Emergency Recovery Strategy
10) National Public Key Infrastructure (PKI)
11) Public-Private Sector Cybersecurity Collaboration
12) Critical Service Sector CIRTS: Banking, Energy, Transport…

…….The ITU Global Programme is supported through regional CIRT Workshops, Cyber Guidelines, Standards Developments and International Partnerships

ITU WTSA Resolution 58: Establish National CIRTs



ITU WTSA Resolution 58 states the following:

[…]
instructs the Director of the Telecommunication Standardization Bureau, in collaboration with the Director of the Telecommunication Development Bureau

1) to identify best practices to establish CIRTs;
2) to identify where CIRTs are needed;
3) to collaborate with international experts and bodies to establish national CIRTs;
4) to provide support, as appropriate, within existing budgetary resources;
5) to facilitate collaboration between national CIRTs, such as capacity building and exchange of information, within an appropriate framework,

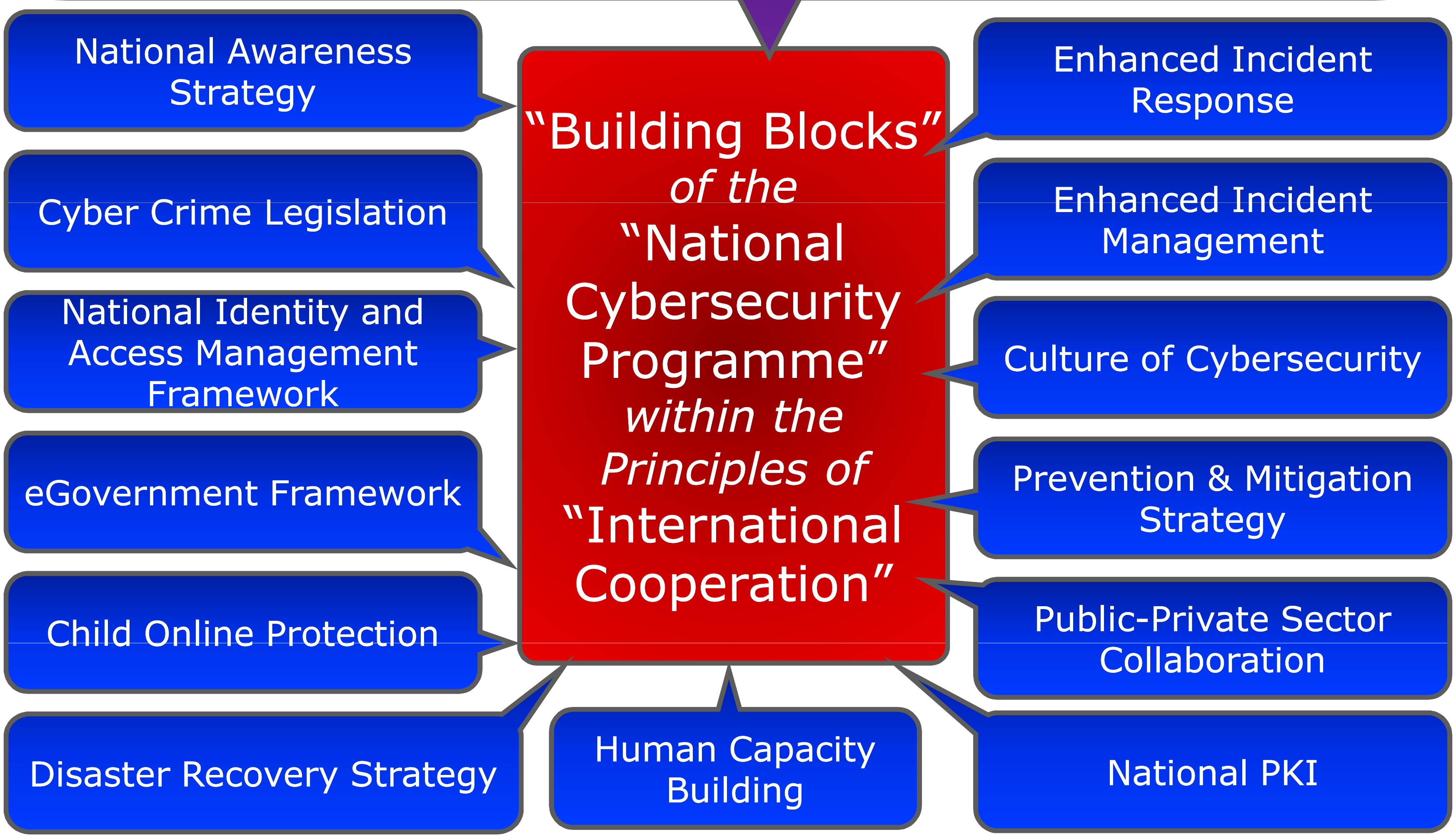
invites the Member States

1) to consider the creation of a national CIRT as a high priority;
2) to collaborate with other Member States and with Sector Members,

[…]

[See the full text of ITU WTSA Resolution 58…]

ITU : Business Benefits from CIRTs….



“Building Blocks” *of the* “National Cybersecurity Programme” *within the Principles of* “International Cooperation”

National Awareness Strategy

Cyber Crime Legislation

National Identity and Access Management Framework

eGovernment Framework

Child Online Protection

Disaster Recovery Strategy

Human Capacity Building

Enhanced Incident Response

Enhanced Incident Management

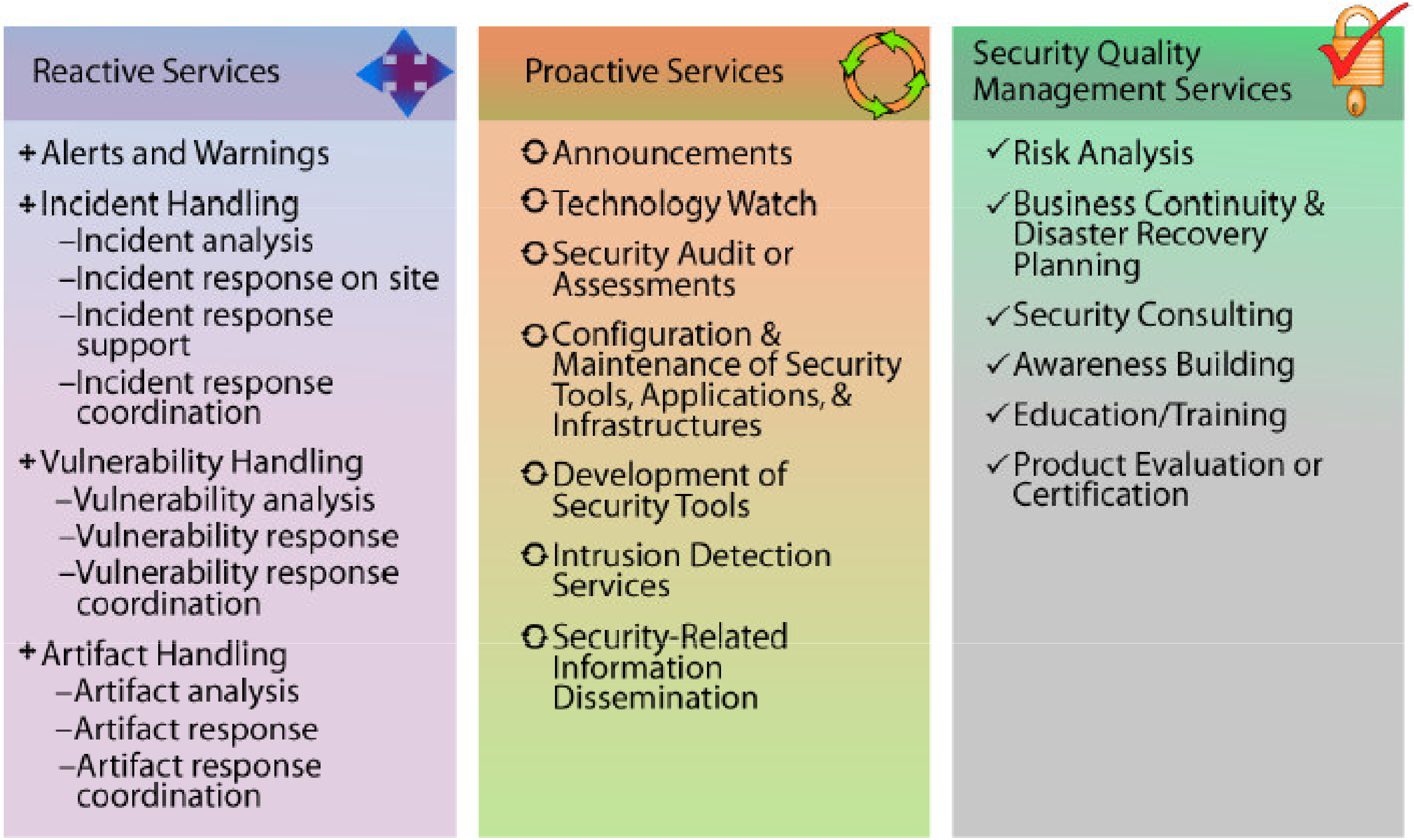
Culture of Cybersecurity

Prevention & Mitigation Strategy

Public-Private Sector Collaboration

National PKI

CERT/CIRT 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

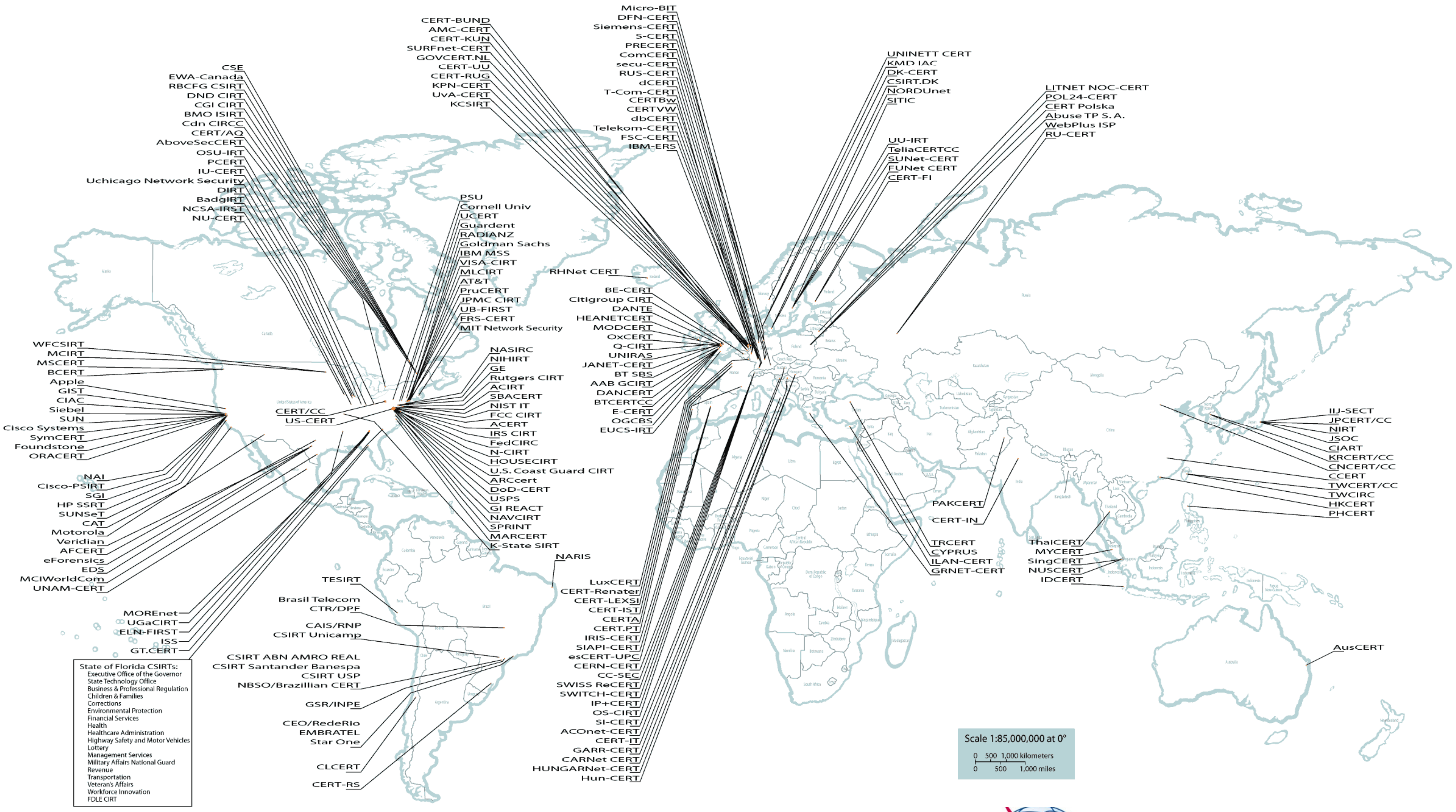
ITU-IMPACT: Global Response Centre

Business CIRT: Integrated Command & Control

- Security Operations Command Centre for Global Security Software Enterprise

Incident Response Teams Around the World

International cooperation speeds response to Internet security breaches.



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

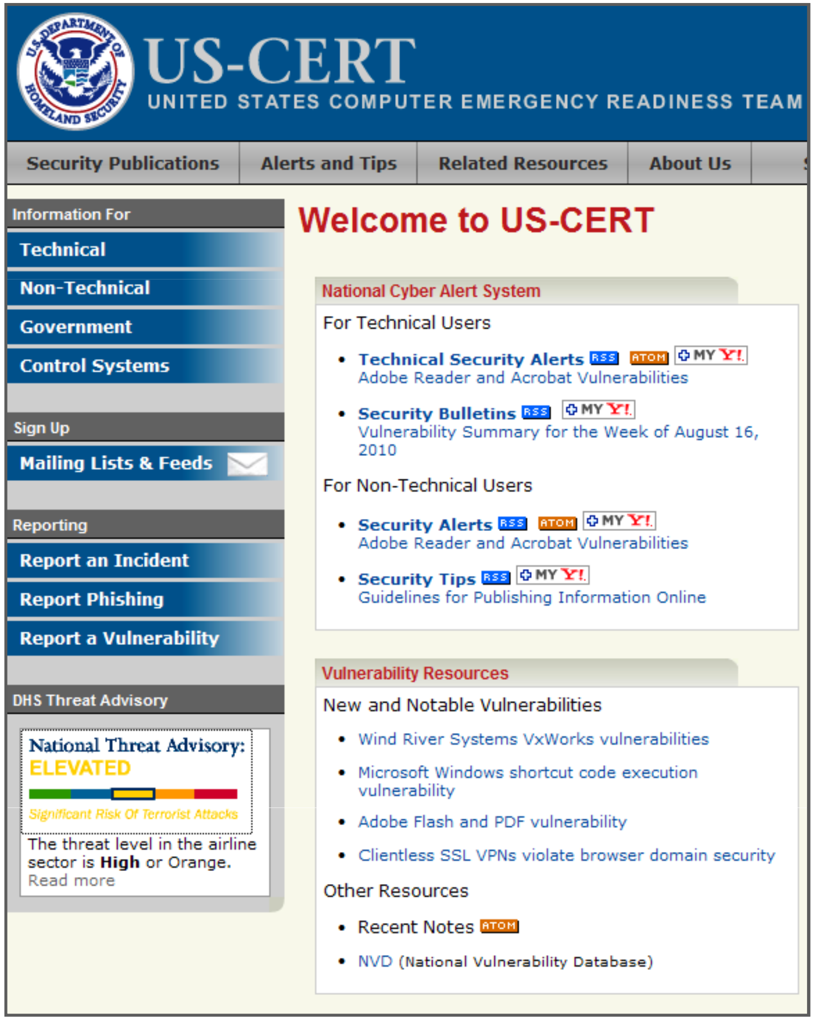
ITU AND CITEL REGIONAL CYBERSECURITY CAPACITY BUILDING WORKSHOP FOR THE AMERICAS

Monday 1st November 2010, Salta City, Argentina

International Telecommunication Union

Committed to connecting the world

US and Asia-Pacific CERTs



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Security Publications | Alerts and Tips | Related Resources | About Us

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

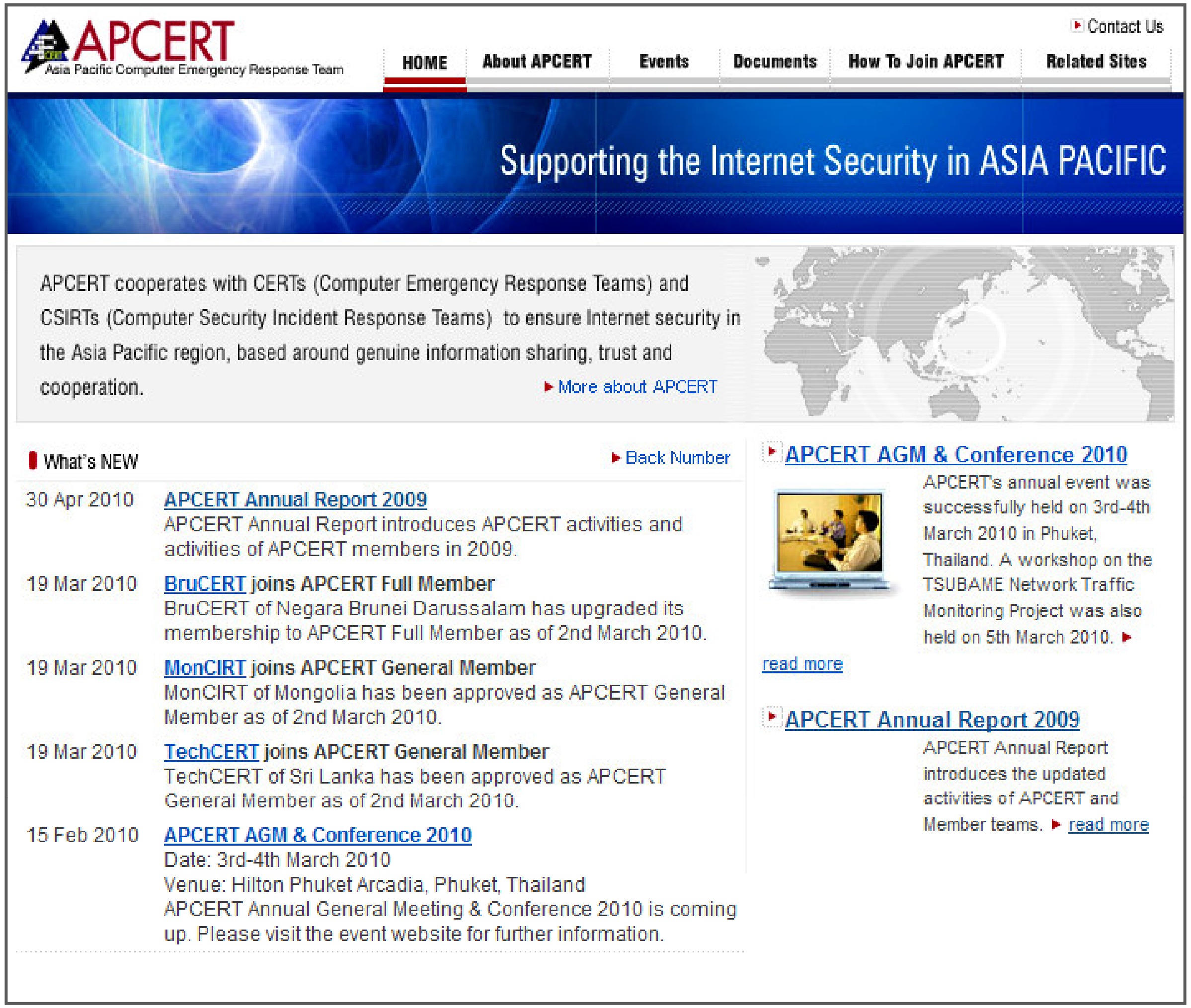
For Technical Users
- **Technical Security Alerts** RSS ATOM MY Y!
  Adobe Reader and Acrobat Vulnerabilities
- **Security Bulletins** RSS MY Y!
  Vulnerability Summary for the Week of August 16, 2010

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

Contact Us

HOME | About APCERT | Events | Documents | How To Join APCERT | Related Sites

Supporting the Internet Security in ASIA PACIFIC

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

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

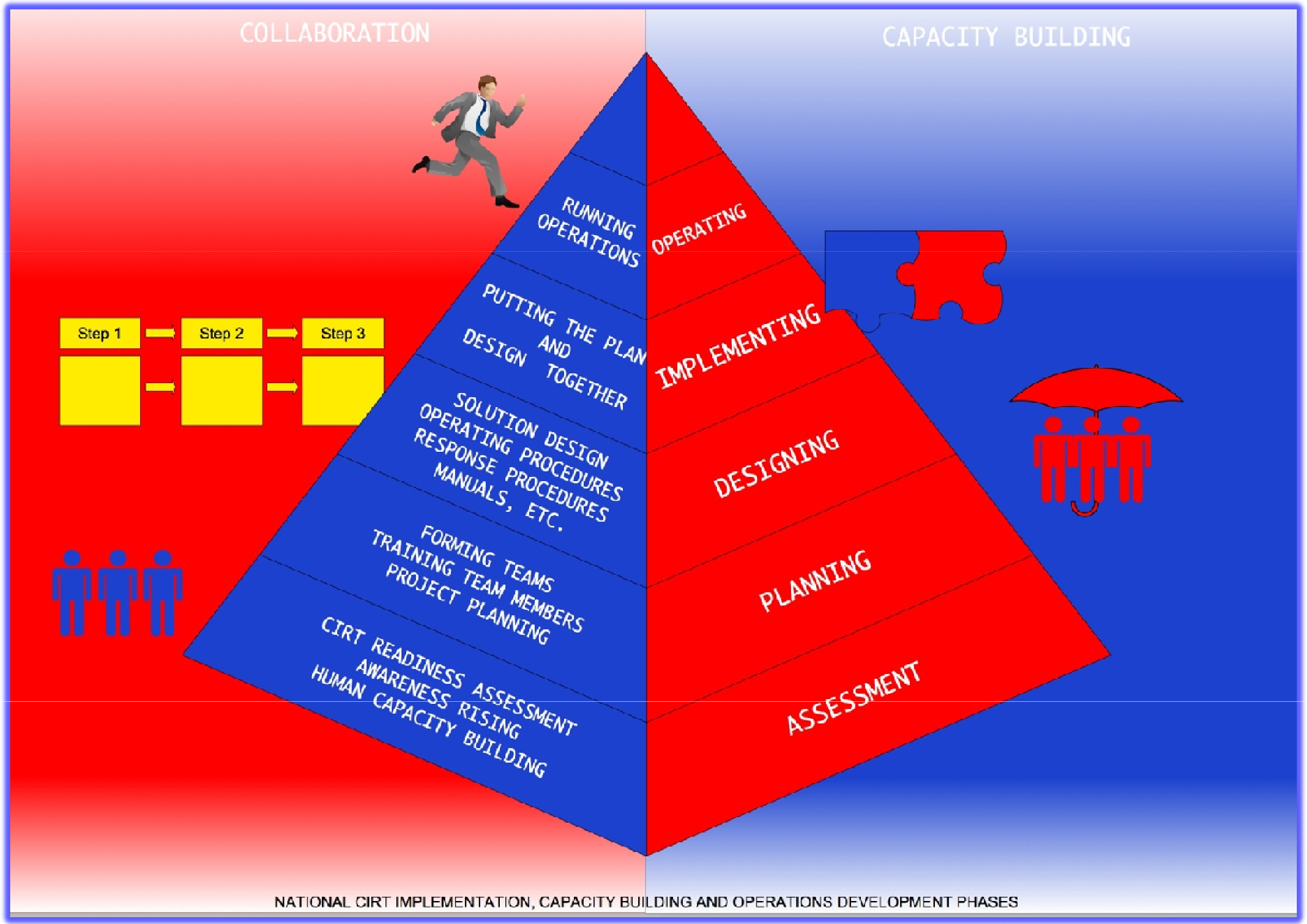
International Telecommunication Union
Committed to connecting the world

Selected Latin American CERTs

- Argentina:
  - ArCERT – Argentina Public Administration– *arcert.gov.ar*
  - CSIRT BANELCO – Banking Sector including Standard Bank & Santanderrio
- Brazil:
  - CAIS/RNP – Brazilian Academic & Research Network- *cais.rnp.br*
  - CERTbr – Brazilian Internet Steering Committee – *cert.br*
- Chile:
  - CLCERT – Chilean Government CERT – *clcert.cl*
- Mexico:
  - UNAM-CERT – National Autonomous University of Mexico – *unam-cert.unam.mx*
- Peru:
  - TERIS – Telefonica Security Incident CERT – *tp.com/teris and tp.com.pe/security*
- Uruguay:
  - CSIRT ANTEL – National Telecomms Administration – *csirt-antel.com.uy*
- Venezuala:
  - VenCERT – Venezualan Government CERT – *vencert.gob.ve*

Source: www.FIRST.org

ITU: National CIRT Implementation Framework

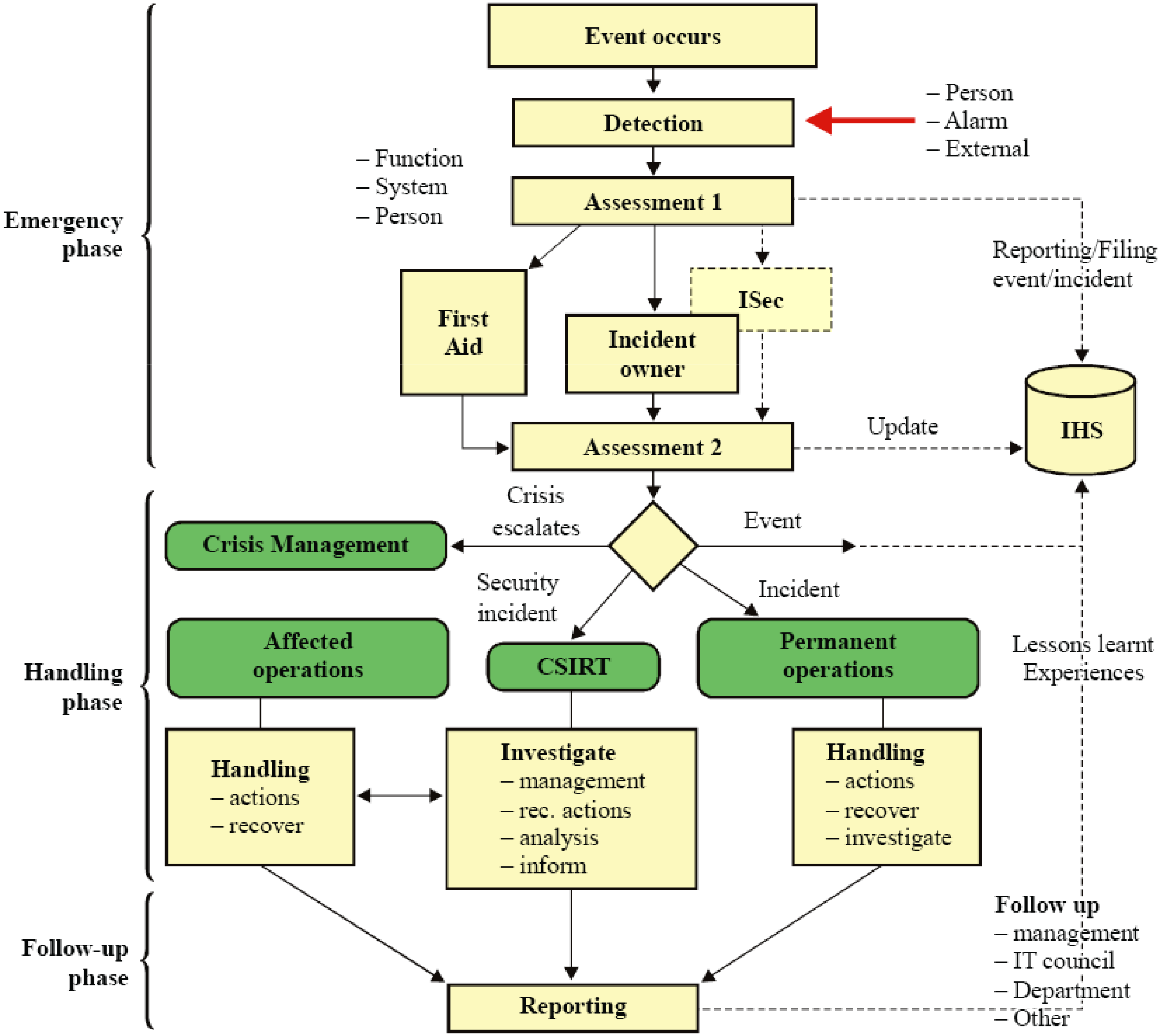


National CIRT Alert Centre

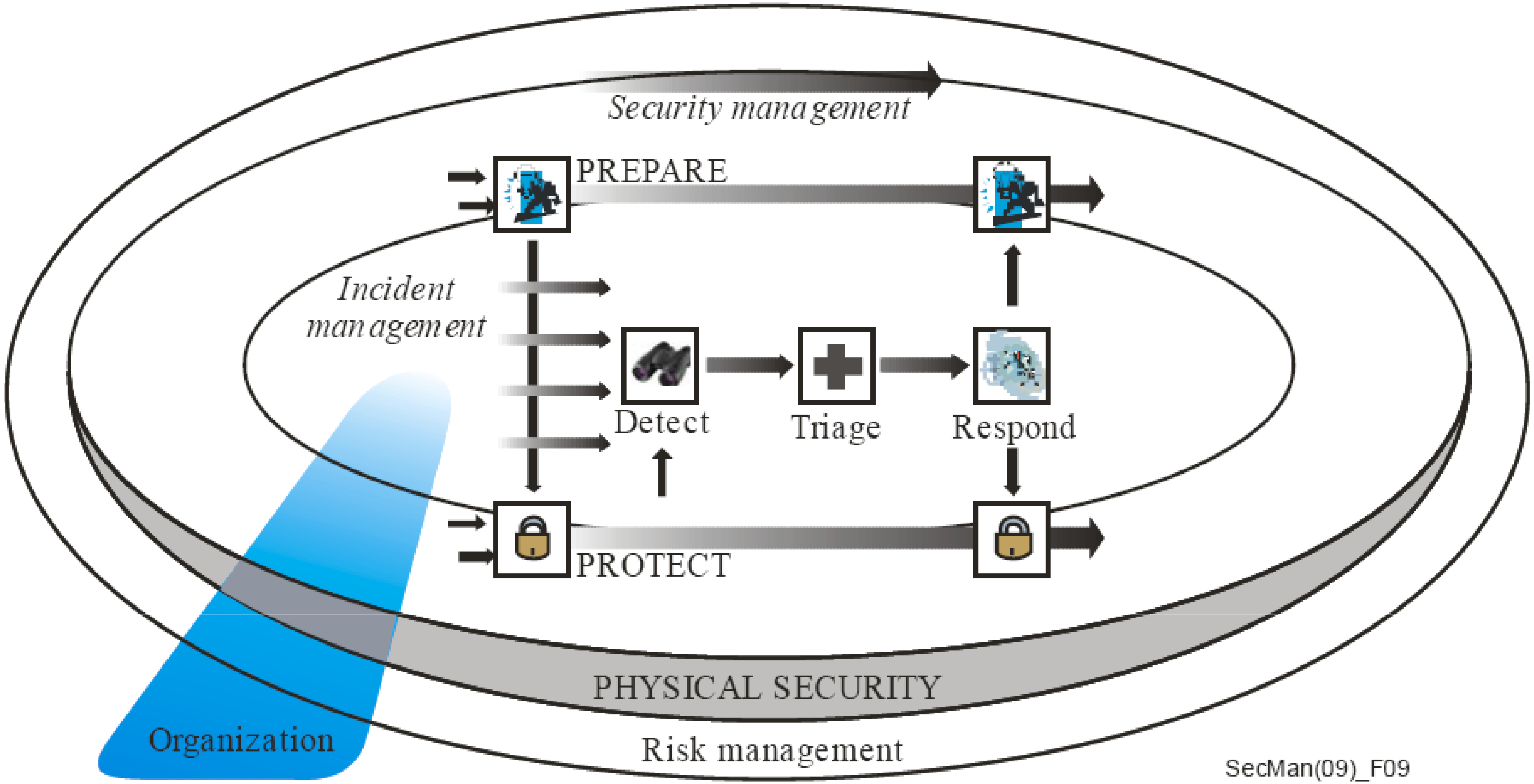
- *Alerts:* A Fundamental Process within any CERT is the management and classification of "incidents", and their routing to provide a response
- *Triage:* Some "incidents" may actually be due to some unusual statistical traffic patterns rather than an actual alert, "hack" or cybercrime
- *Risk:* Once 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 slides show this incident process flow in more detail…

Critical Events: Incident Flows – ITU:E.409



Comparison of Security Management & Incident Management: ITU – X.1056



SecMan(09)_F09

Cybersecurity Organisational Structures & Incident Management for CITEL-OAS

1 –Aim: National Cybersecurity	2 – Critical Service Sectors	3 – Cyber Attack Scenarios
4–"Best Practice" Case Studies	5–CIRT: Organisational Models	6 – The "Cyber" Business Case
7 – Global IMPACT Alliance	8 - Public-Private Partnership	9 – Next Suggested Steps

Cybersecurity Costs : Short-Term

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

Annual Cybersecurity Budgets

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

- Annual Security Budgets will need to include allowances for:
  - Staff salaries & operational costs for the CIRT & National Cybersecurity Agency
  - Costs for tackling cybercrime through a possible National Cybercrime Unit
  - Management of cybersecurity by National & Regional Civilian Authorities
  - Costs of required annual security audits to ensure ongoing compliance
  - Professional training courses at leading Educational Colleges & Universities
  - Costs for maintaining "best practice" cybersecurity within each of the critical service sectors within your National Economies such as Telecomms & Banking
  - Regular Systems, Computing & Communications reviews & upgrades for all secure government computing centres, as well as those for major enterprises
  - On-going costs top support extensive international partnerships & collaboration

Cybersecurity Benefits: Government

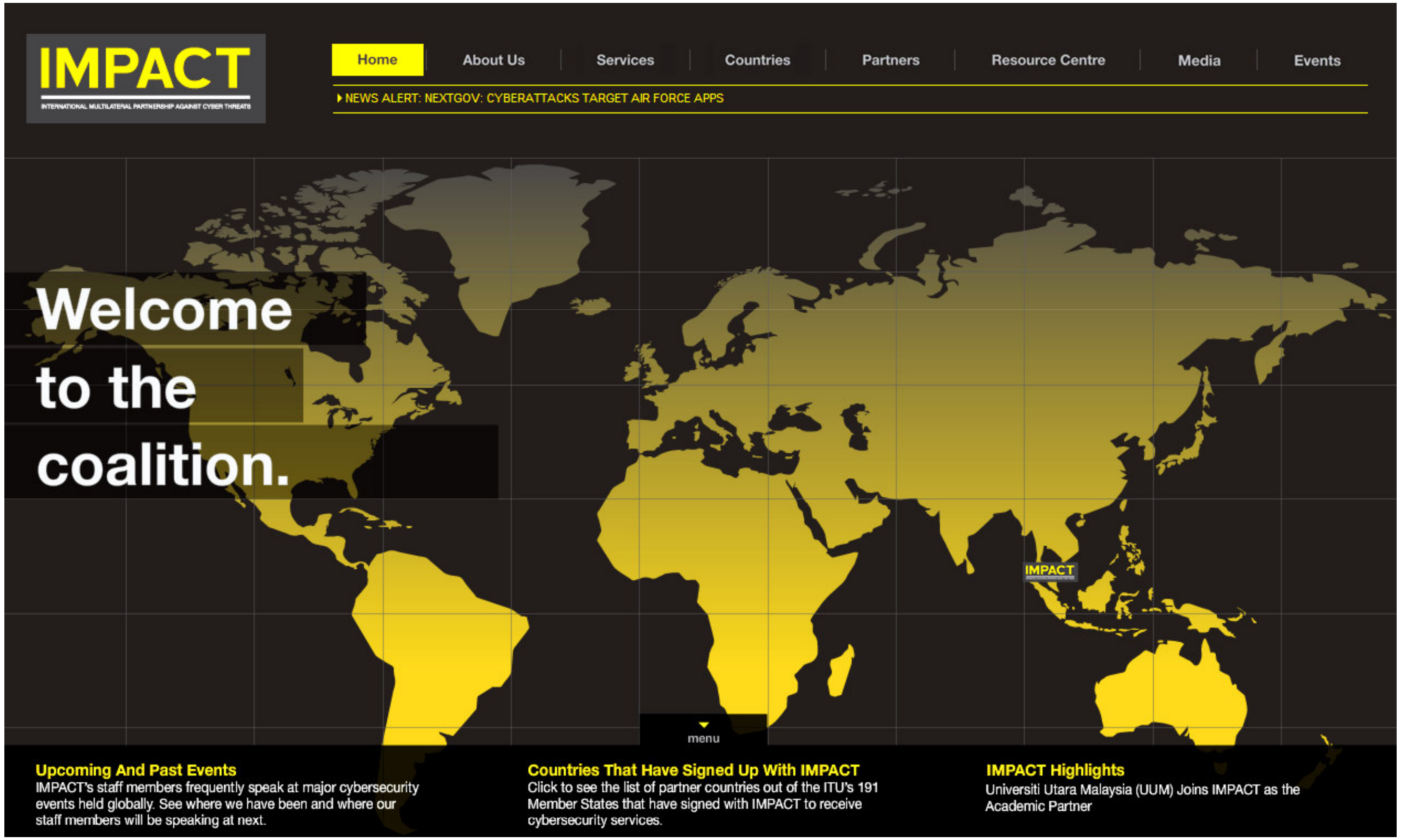
- Improved cybersecurity provides significant benefits to the Government & Critical National Service Sectors including:
  - *eGovernment:* Fully secure & cost effective delivery of on-line services to both citizens and businesses, such as taxes & customs, social welfare, civil & land registries, passports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

Cybersecurity Organisational Structures & Incident Management for CITEL-OAS

1 –Aim: National Cybersecurity	2 – Critical Service Sectors	3 – Cyber Attack Scenarios
4–"Best Practice" Case Studies	5–CIRT: Organisational Models	6 – The "Cyber" Business Case
7 – Global IMPACT Alliance	8 - Public-Private Partnership	9 – Next Suggested Steps

IMPACT : Worldwide Cybersecurity Alliance

IMPACT International Partners: **ITU**, UN, INTERPOL and CTO



▸ NEWS ALERT: NEXTGOV: CYBERATTACKS TARGET AIR FORCE APPS

Welcome to the coalition.

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

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

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

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

IMPACT = International Multilateral Partnerships Against Cyber Threats

ITU : IMPACT Cybersecurity Programmes

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

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

- 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 membership 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.

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 Honey Pot
10) Cyber Threat Route Plotter

IMPACT

INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

Cybersecurity Organisational Structures & Incident Management for CITEL-OAS

1 –Aim: National Cybersecurity	2 – Critical Service Sectors	3 – Cyber Attack Scenarios
4–"Best Practice" Case Studies	5–CIRT: Organisational Models	6 – The "Cyber" Business Case
7 – Global IMPACT Alliance	8 - Public-Private Partnership	9 – Next Suggested Steps

Public – Private Partnerships (PPP) : Development of CyberSecurity Skills

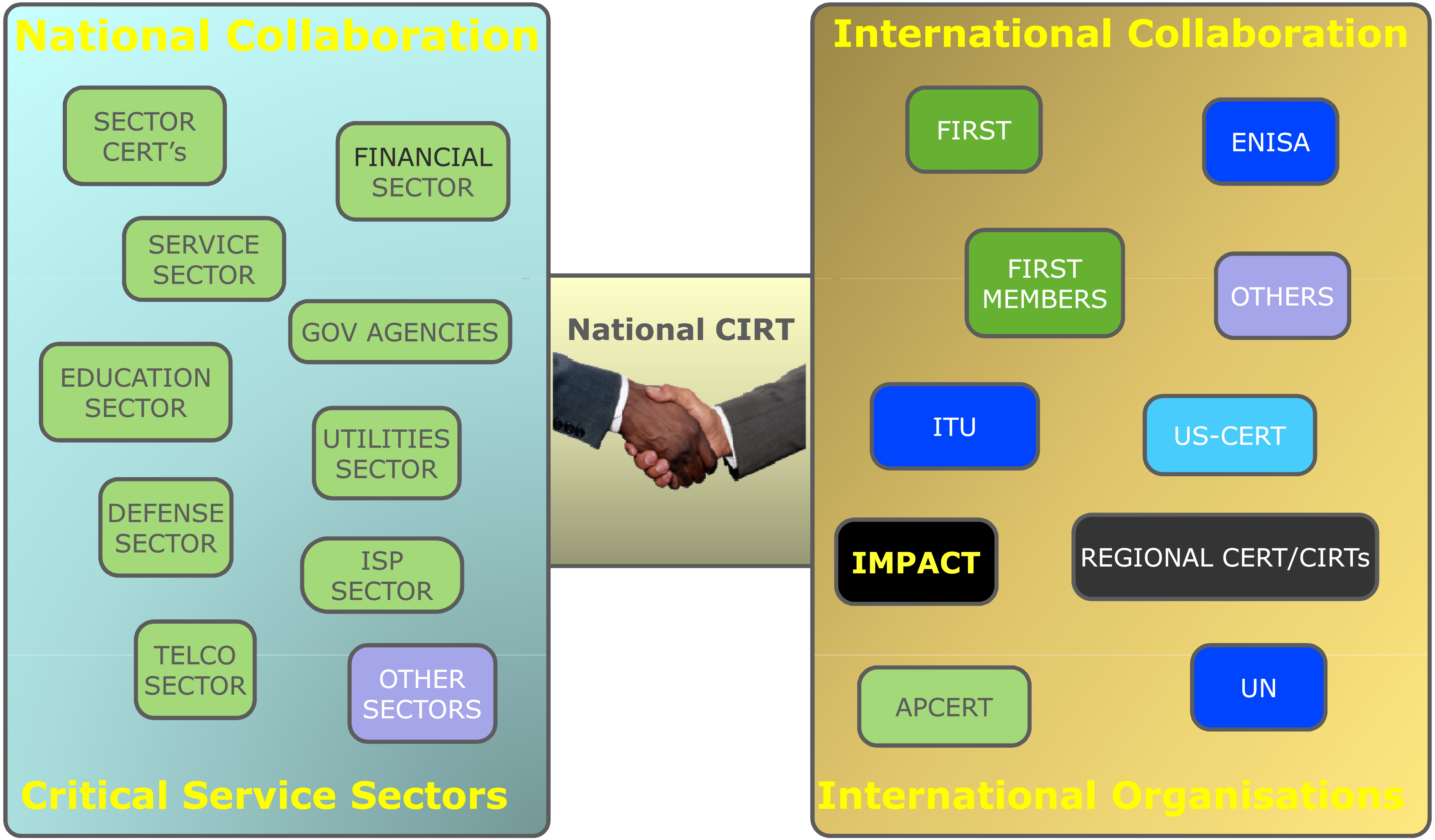
- The extensive scope required for cybersecurity capacity & skills building mean that a recommended way forward is for the government to negotiate partnerships with the private business sector

- The PPP Model is used extensively in many countries in which the government outsources ICT-based eGov services and training to private sector companies that already have the requisite skills:

  - CERT/CSIRTs may be outsourced to Telecomms/ISPs as well as the University Networks
  - Government ICT Infrastructure, and eGov Applications Hosting can also be outsourced
  - Awareness and Professional Training can be managed through Colleges & Universities
  - Critical Service Sector Skills Building for Cybersecurity will be developed in partnership with the relevant sector such as banking/finance, energy, agriculture, travel and tourism

- Using PPP will significantly accelerate the rate at which your Government Administration can implement its cybersecurity action plan & roadmap whilst at the same time sharing the investment cost with business.

CIRT Deployment: Public-Private International Collaboration



National Collaboration

SECTOR CERT’s

FINANCIAL SECTOR

SERVICE SECTOR

GOV AGENCIES

EDUCATION SECTOR

UTILITIES SECTOR

DEFENSE SECTOR

ISP SECTOR

TELCO SECTOR

OTHER SECTORS

Critical Service Sectors

National CIRT

International Collaboration

FIRST

ENISA

FIRST MEMBERS

OTHERS

ITU

US-CERT

IMPACT

REGIONAL CERT/CIRTs

APCERT

UN

International Organisations

Cybersecurity Organisational Structures & Incident Management for CITEL-OAS

1 –Aim: National Cybersecurity	2 – Critical Service Sectors	3 – Cyber Attack Scenarios
4–"Best Practice" Case Studies	5–CIRT: Organisational Models	6 – The "Cyber" Business Case
7 – Global IMPACT Alliance	8 - Public-Private Partnership	9 – Next Suggested Steps

Suggested Next Steps for CITEL-OAS Members

- *Review and implement UN Resolution 64/211 (December 2009)* – “Creation of Global Culture of Cybersecurity, including Voluntary Self-Assessment Tool for National Efforts to protect Critical Information Infrastructures” – *Using ITU Guidelines & Toolkits*

- *Appoint Top-Level Cybersecurity Team* to review current status of cybersecurity within the Government, Telecomms & designated Critical Information Service Sectors using *ITU’s GCA 5 Pillars of Legal, Technical, Organisational, Capacity & Partnerships*

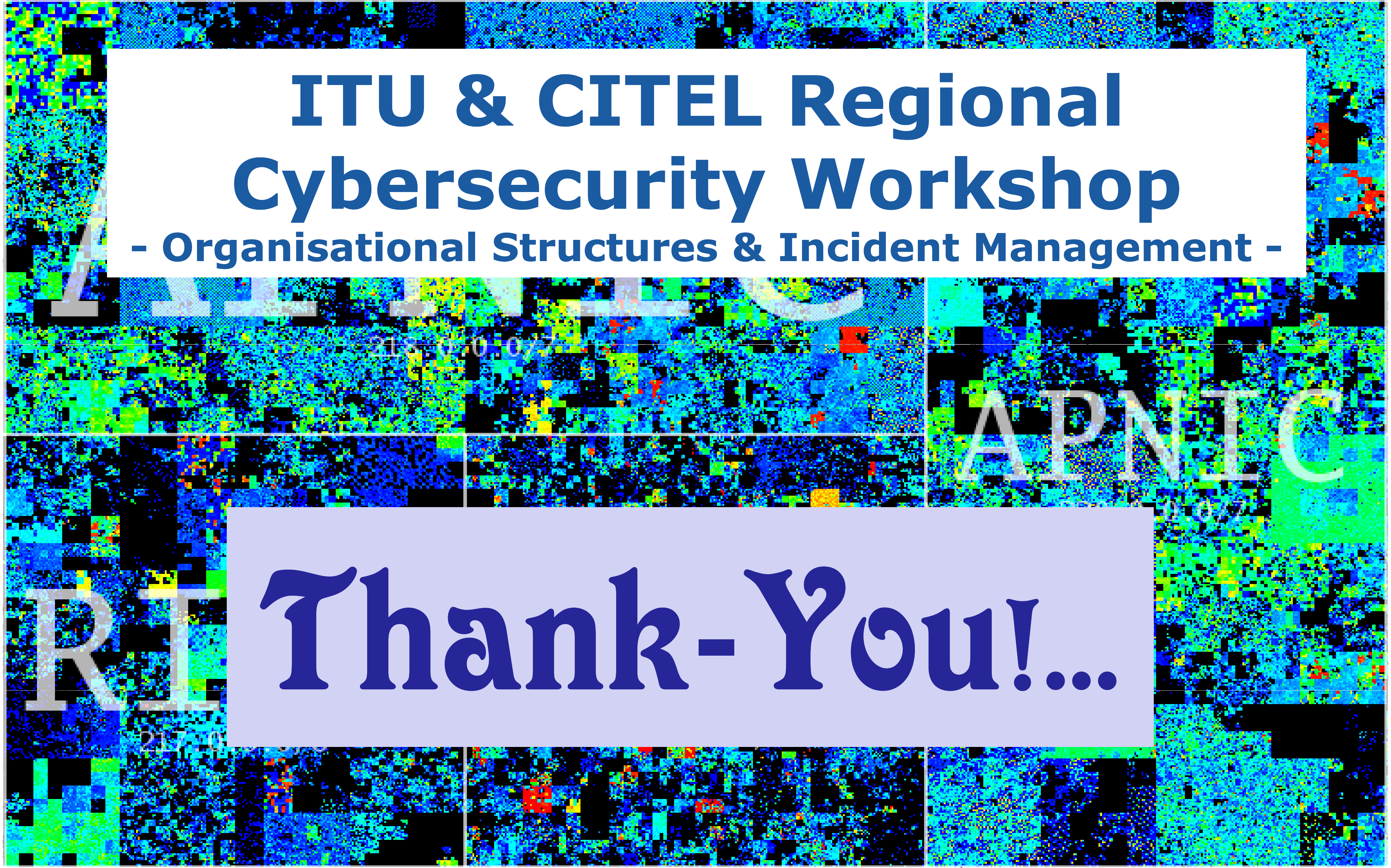
- *Establish a National CIRT and National Government Cybersecurity Agency* (or Council) with authority and budget for the following suggested short to mid-term actions:

1- Cyber Alerts (CIRT): Manage the National Incident Response to Cyber Alerts, and Attacks
2- Critical Sectors: Co-ordination of National Programmes for Critical Information Infrastructure
3- Education & Awareness: Co-ordination of the National Awareness & Cyber Skills Training
4- Legislation: Leadership role in the development of new cyber legislation & regulations
5- Cybercrime Unit: Facilitation for the establishment of a National Cybercrime e-Crime Unit
6- Security Standards: Setting the national cybersecurity standards and auditing compliance
7- International Partnerships*:* Leadership in the promotion & management of partnerships
8- Research: Support for research & development into cybersecurity technologies & solutions

....These actions will be implemented most effectively through outsourcing actions to Public-Private Partnerships (PPP) that utilise existing professional cyber resources & assets!

ITU & CITEL Regional Cybersecurity Workshop

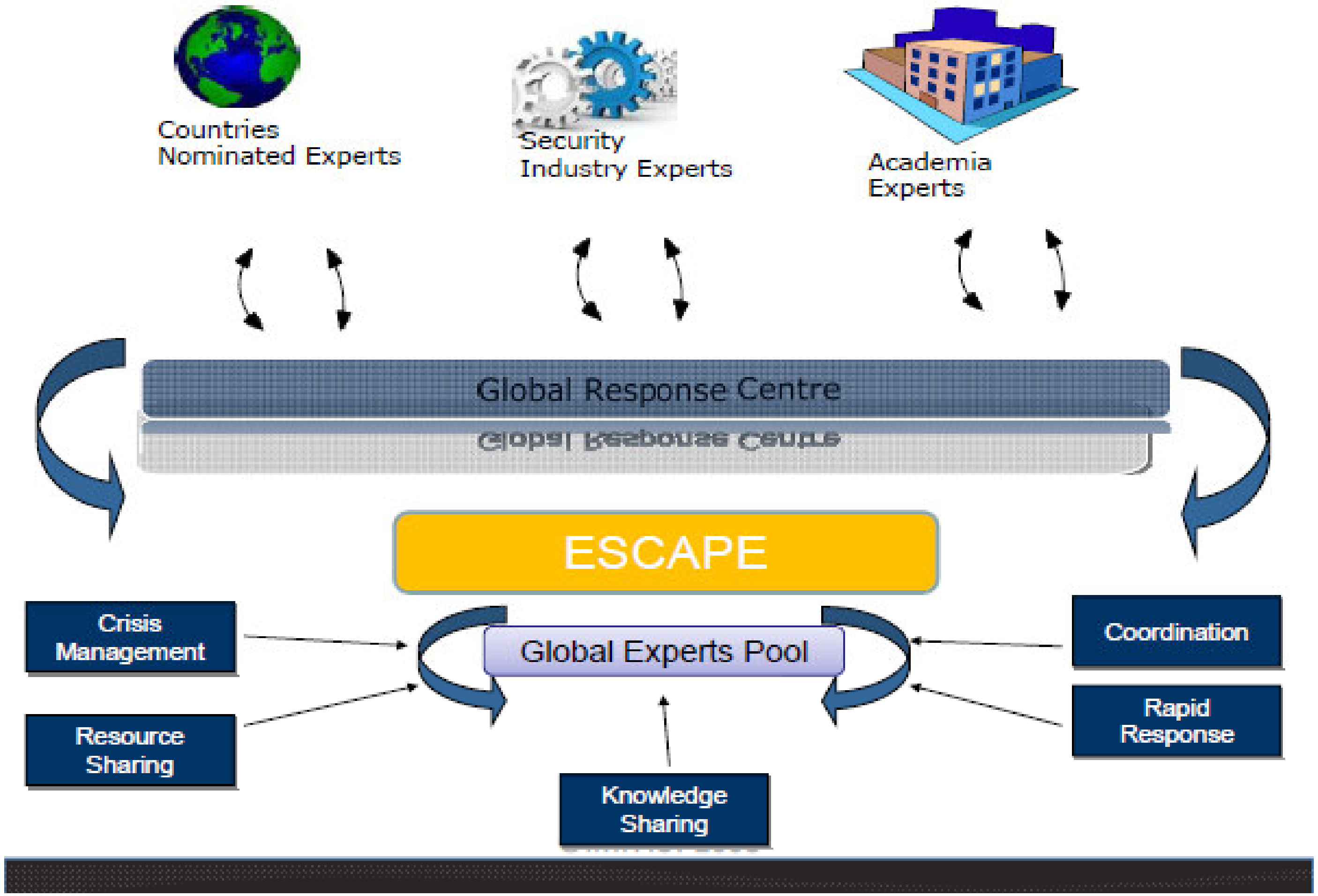
- Organisational Structures & Incident Management -



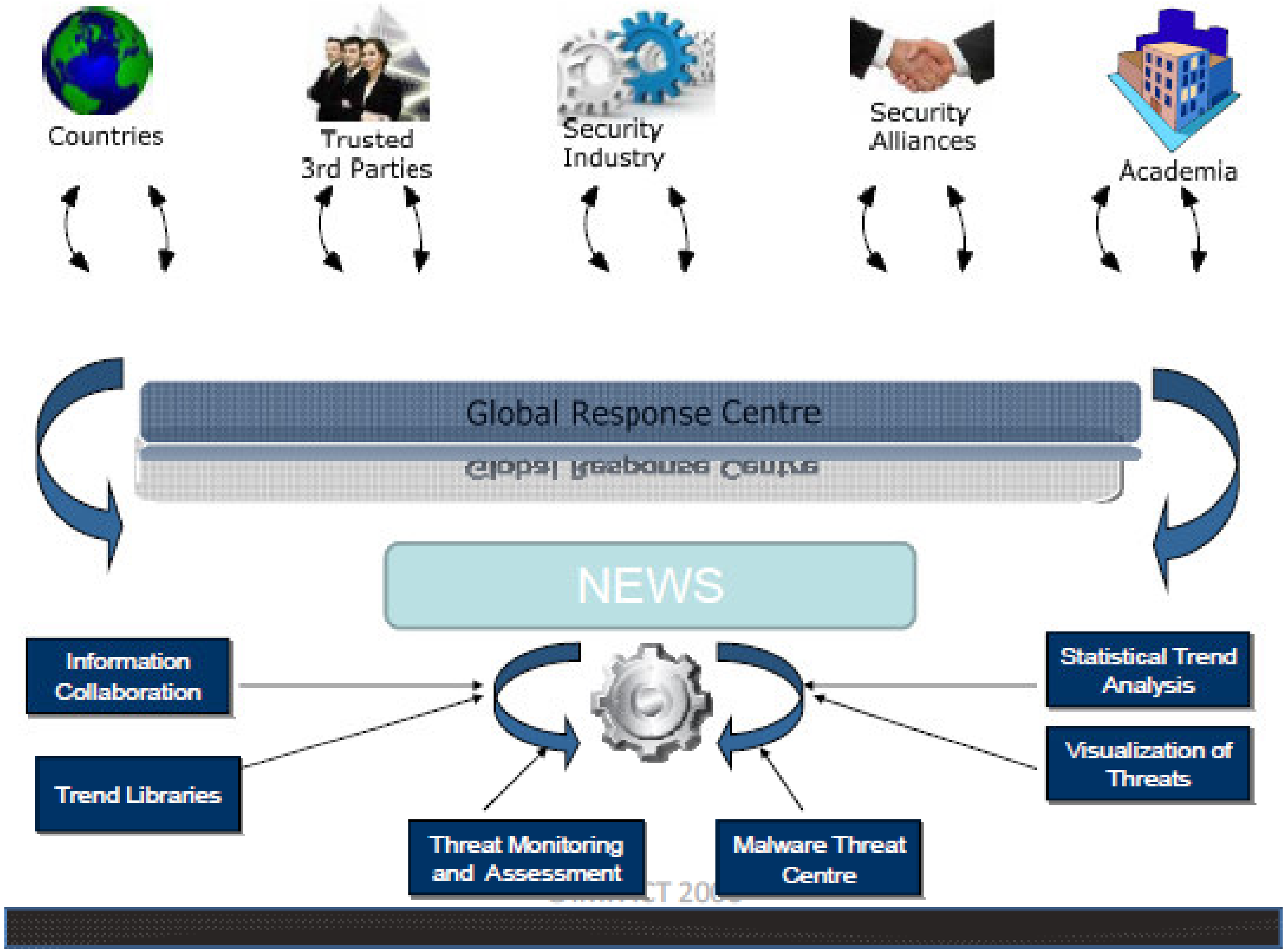
Thank-You!...

BACK-UP SLIDES

Electronically Secure Collaboration Platform for Experts (ESCAPE)



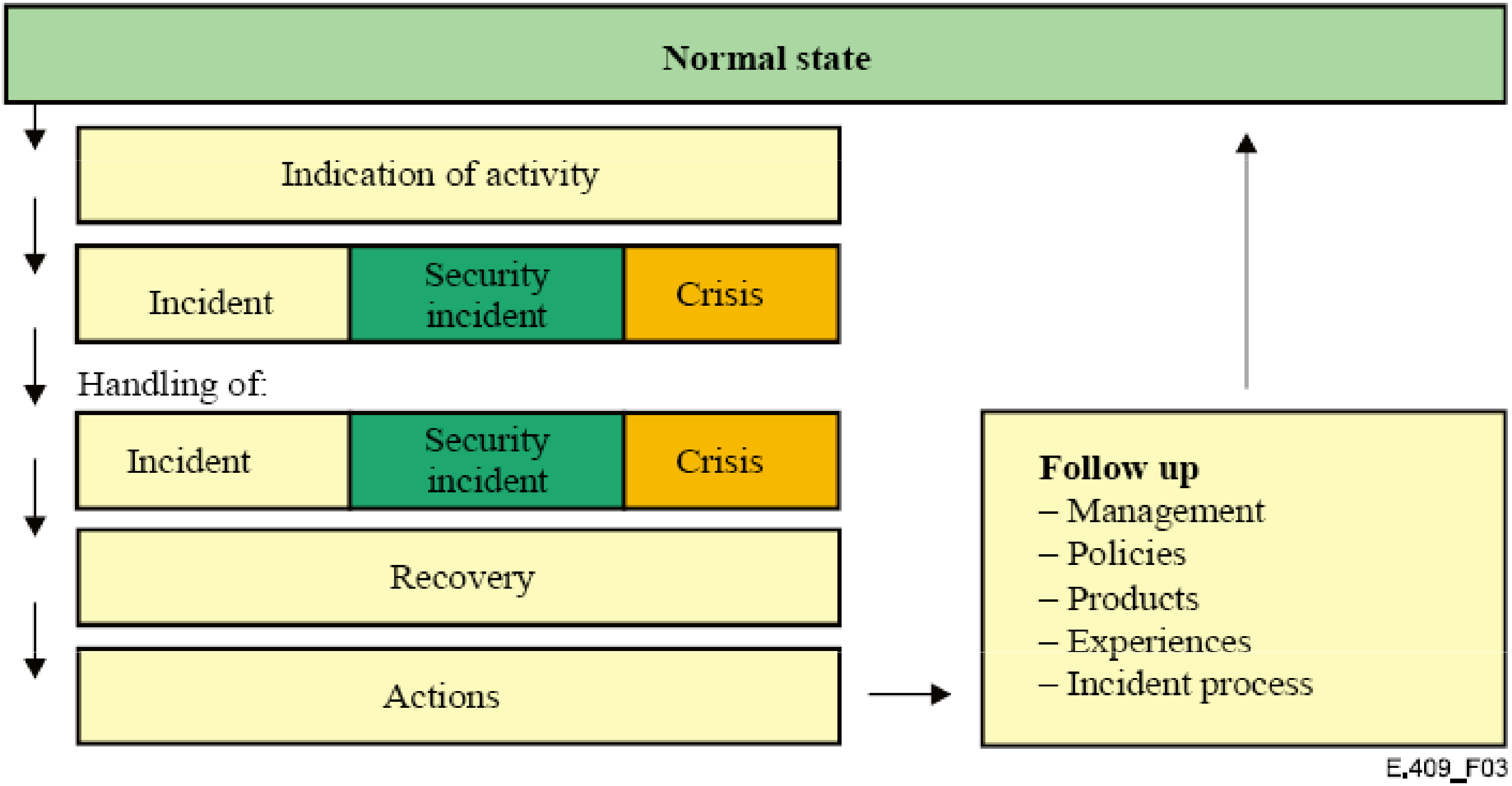
Network Early Warning System(NEWS)



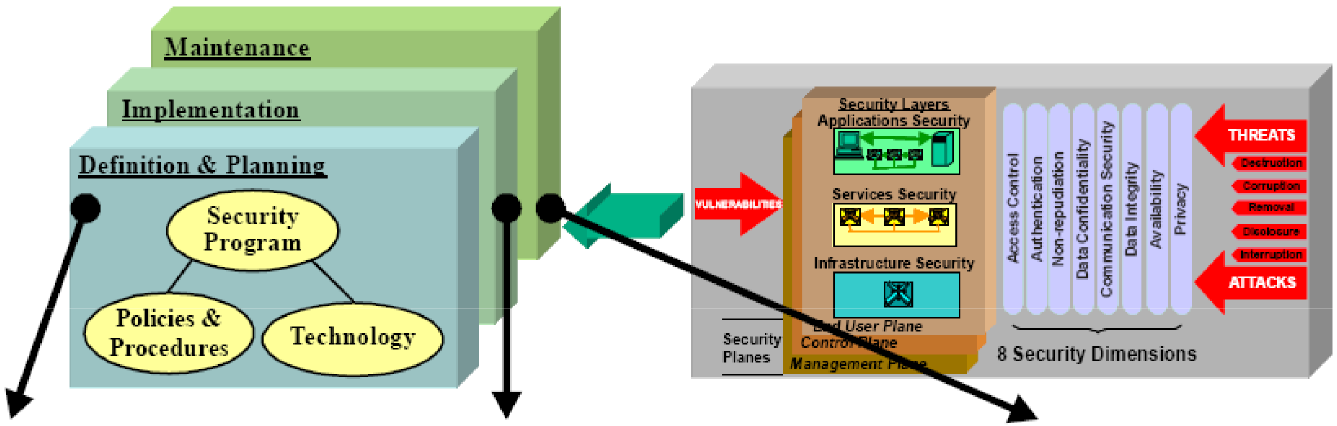
Cyber Threat Sources against Critical National Infrastructure

# Item	THREAT SOURCE NAME	THREAT LEVEL
1	Foreign Intelligence Agencies	Severe
2	Hackers (Individual & National Hackers)	Severe
3	Organised Crime	Severe
4	Unreliable Employees	Moderate
5	Infrastructure Owners and Operators	Moderate
6	Political Activists	Low
7	Investigative Journalists	Negligible

Critical Incident Management



The Life-Cycle of Network Cybersecurity



Definition & planning

Inputs: Business & security objectives, Regulatory & policy specifications, Architecture, Threats

Gap analysis: Compare security objectives, and threats to planned features.

Results: Recommendations to fix gaps, policy compliance

Design & Implementation

Inputs: Product security requirements, technology security practices, design specifications, Threat analysis, Security assets

Gap analysis: Compare results from phase 1, Implemented security features, threat analysis and testing

Results: Security asset identification, vulnerability management, security design compliance and verification, feedback to development process

Deployment & Maintenance

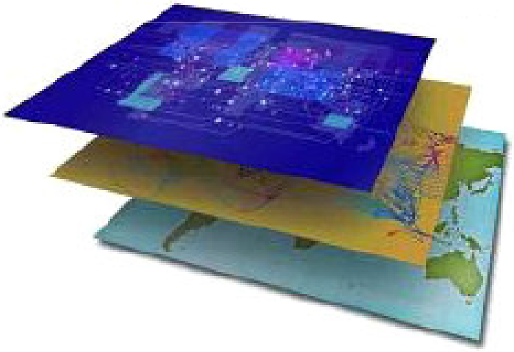
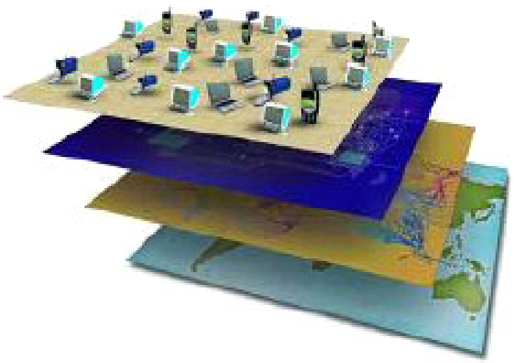
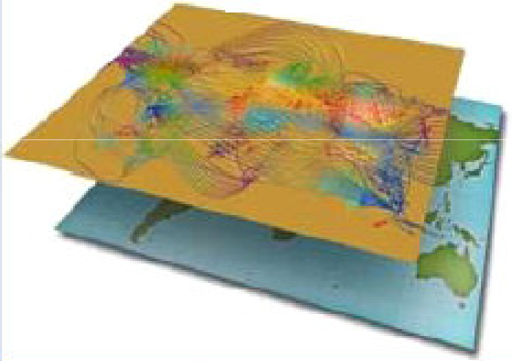
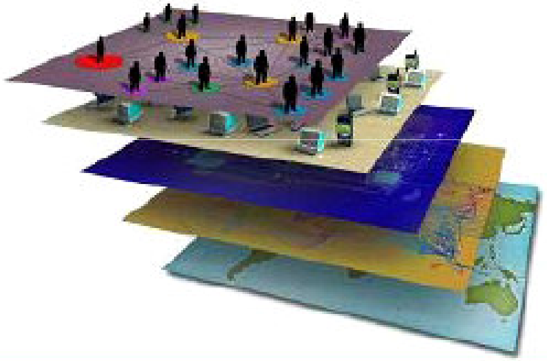
Inputs: Threat & vulnerability management results & updates, Technology and operational security practices, regulatory guidelines

Gap analysis: Compare inputs with product security & operations requirements.

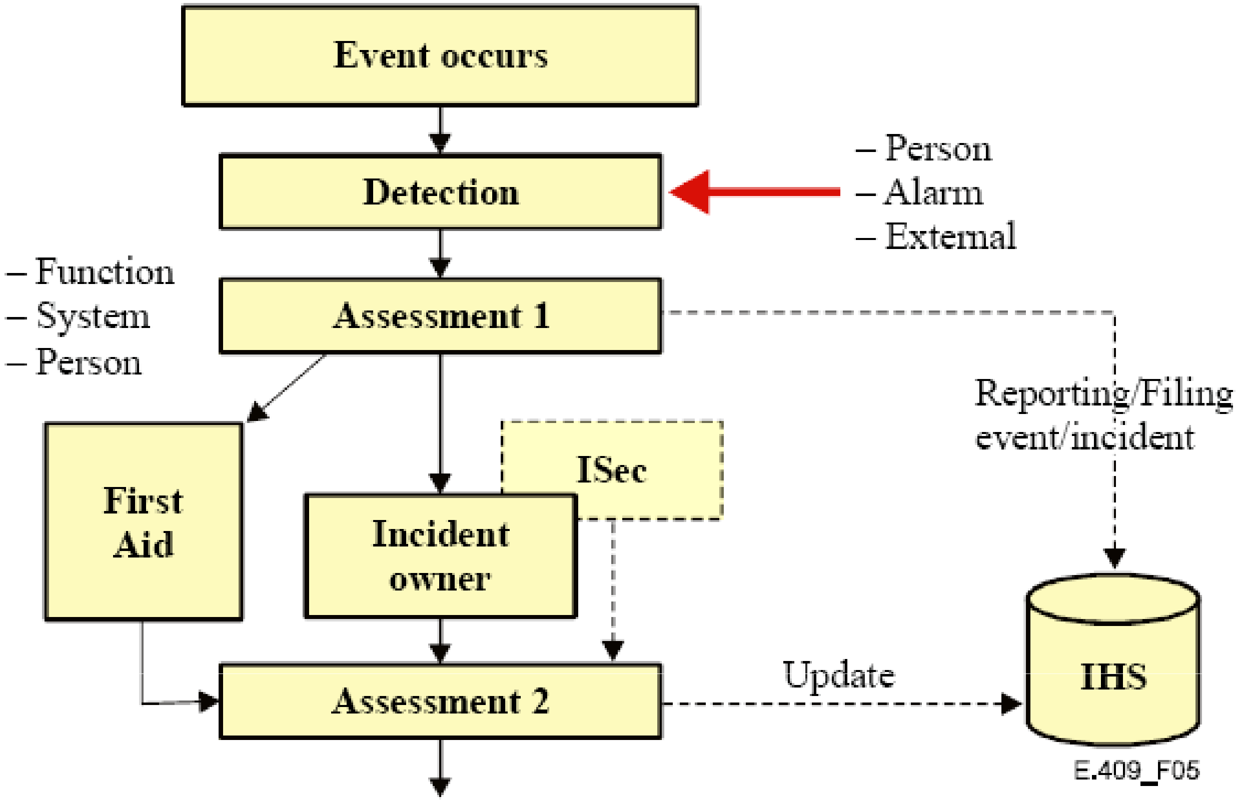
Results: Updated security base line, Feedback to development process

XSuppl.3(08)_F01

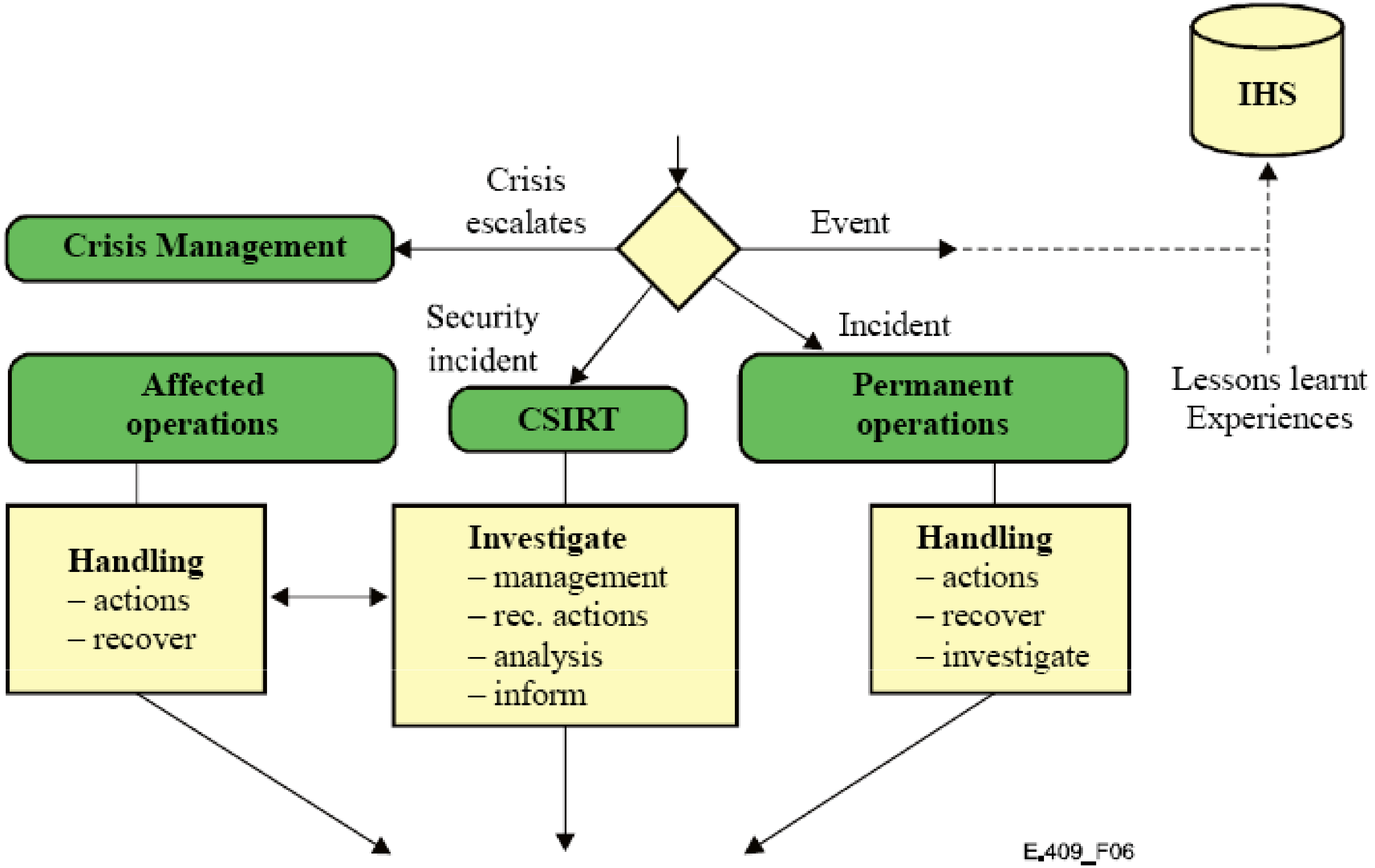
3 Layers of Cyberspace

Physical Layer	Logical Layer	Social Layer
Geographic Components 	Logical Network Components 	Persona Components 
Physical Network Components 		Cyber Persona Components 

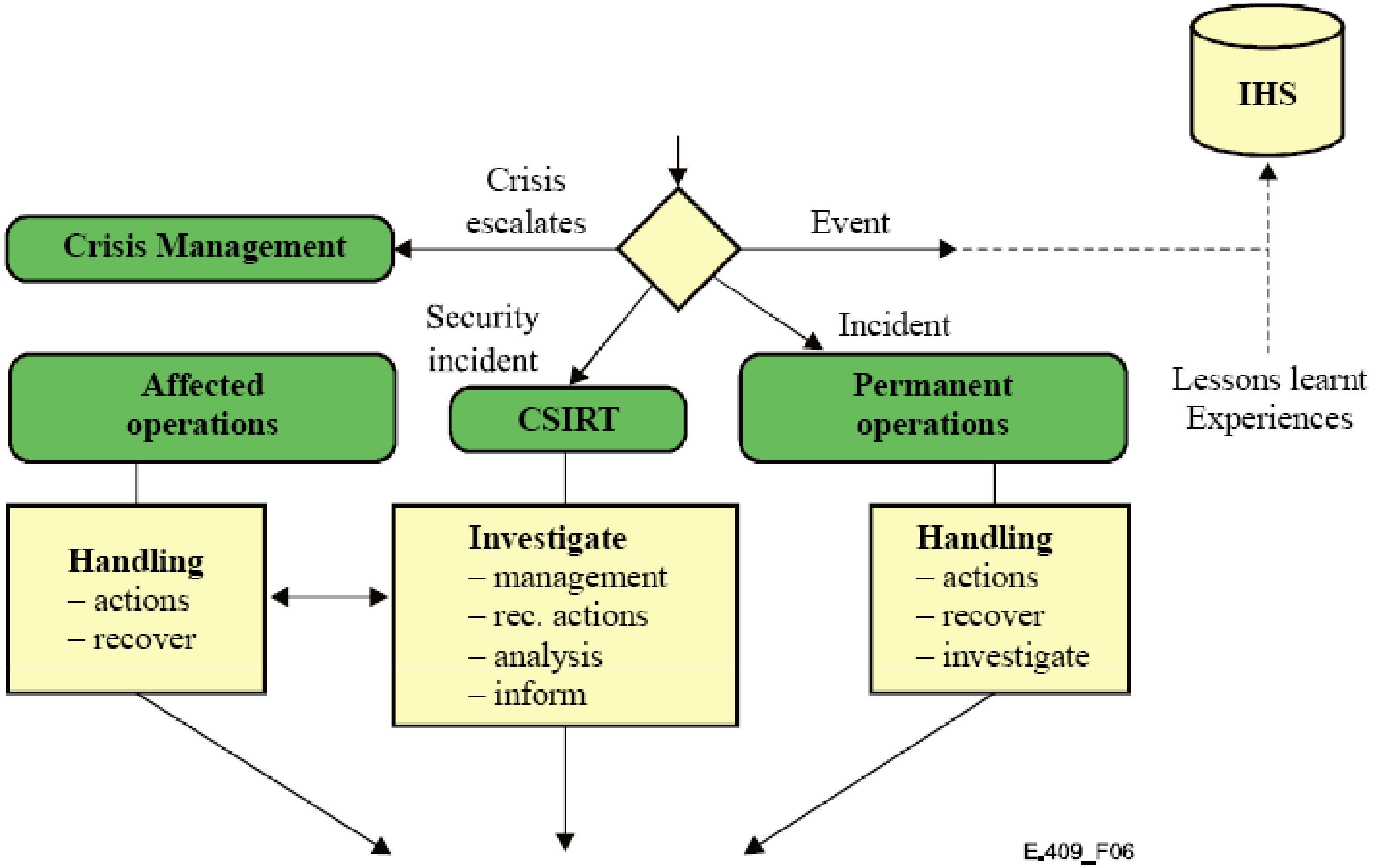
Phase 1 : Emergency Management



Phase 2 : Handling Management



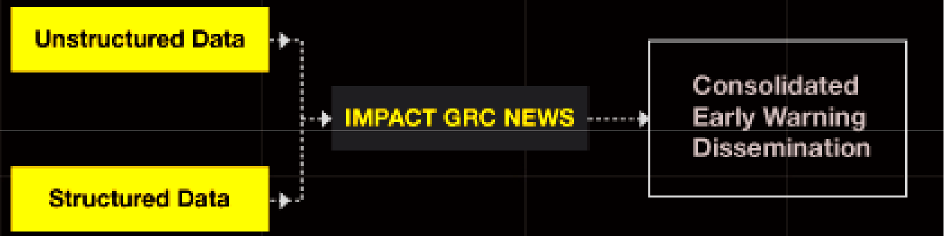
Phase 3 : Follow-Up Activities



IMPACT GRC: NEWS & ESCAPE Programmes

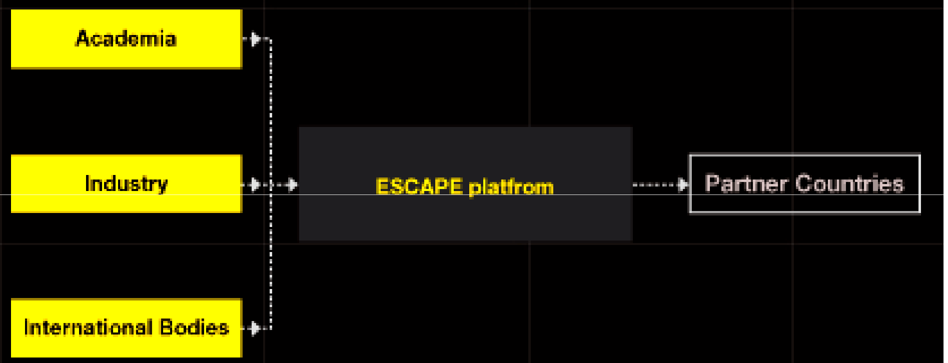
NEWS is a platform of collaborative mashup of information from multiple early warning alliances and cybersecurity vendors. This aims to get the right information to the relevant authorities in a timely manner, enabling them to mitigate and effectively respond to cyber threats that may arise from around 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.



Cyber-Incident Depth Analysis

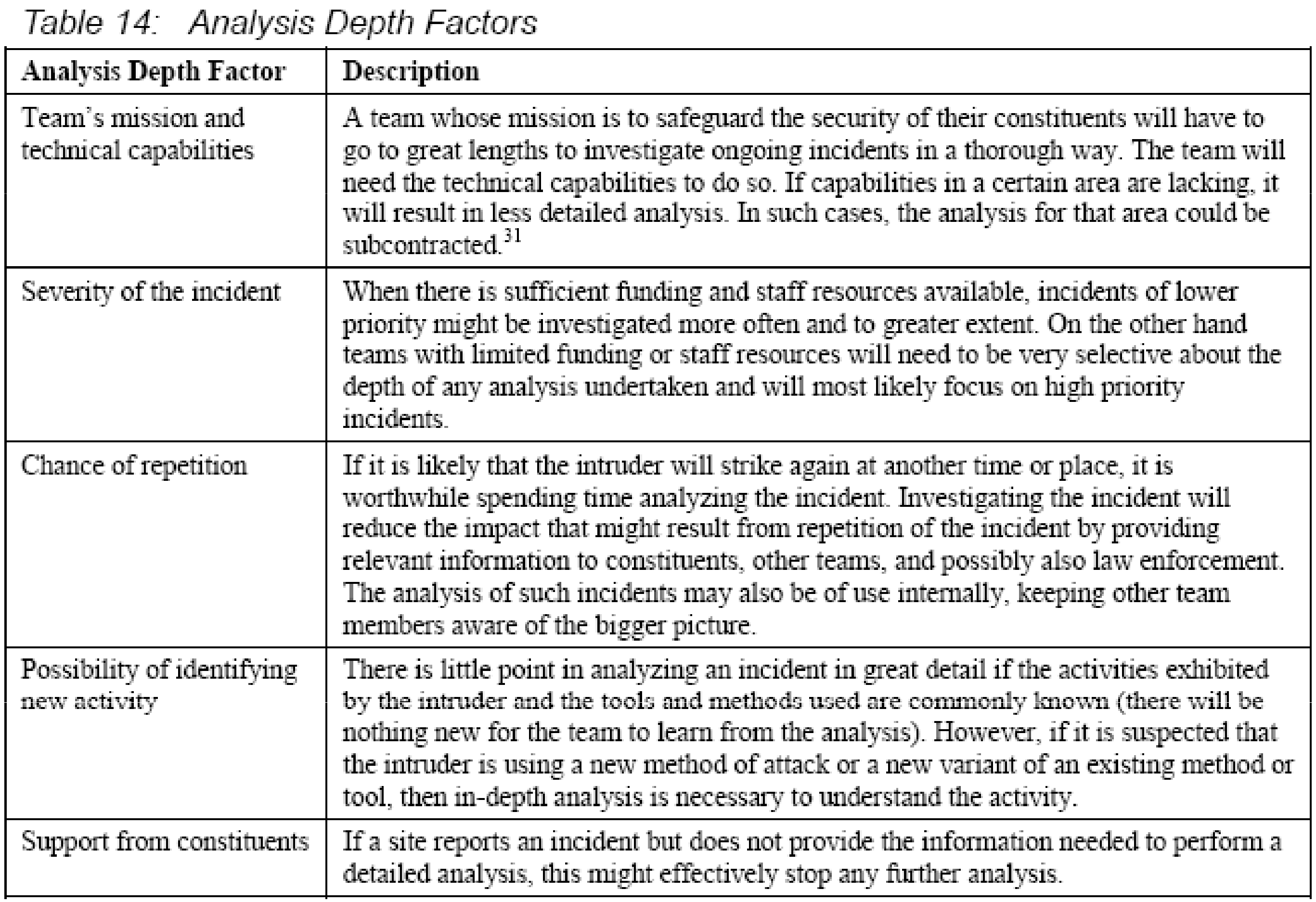


Table 14: Analysis Depth Factors

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.

Worldwide IMPACT Alliance: Organisation

IMPACT

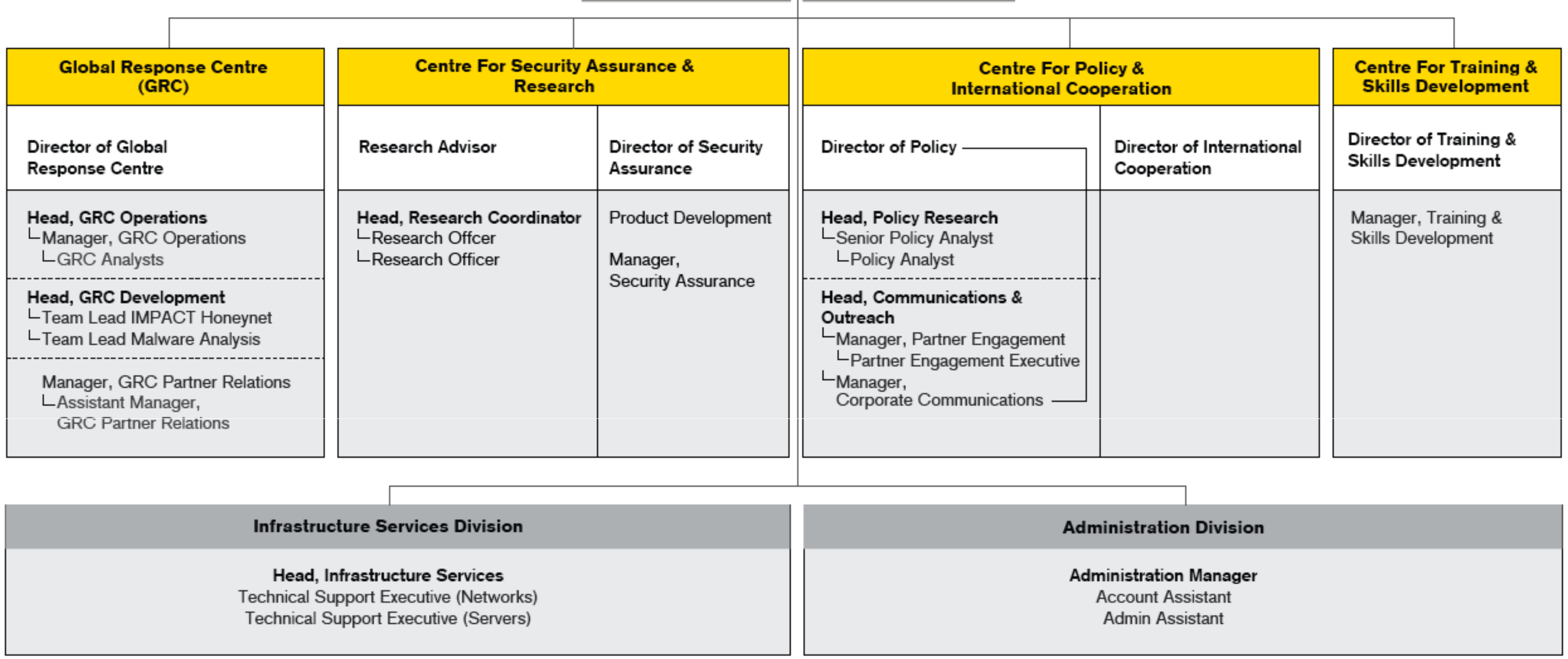
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

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

US Government : Cybersecurity Review

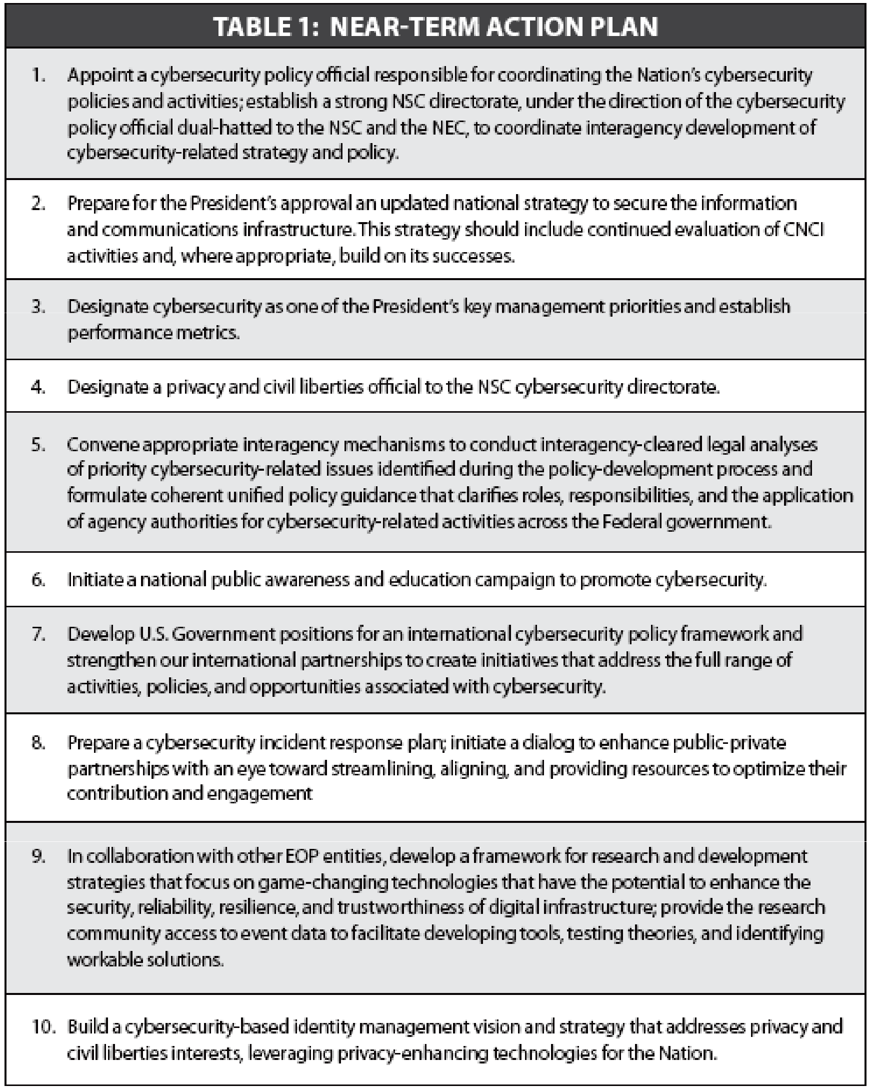


TABLE 1: NEAR-TERM ACTION PLAN
1. Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities; establish a strong NSC directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cybersecurity-related strategy and policy.
2. Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.
3. Designate cybersecurity as one of the President's key management priorities and establish performance metrics.
4. Designate a privacy and civil liberties official to the NSC cybersecurity directorate.
5. Convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government.
6. Initiate a national public awareness and education campaign to promote cybersecurity.
7. Develop U.S. Government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.
8. Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement
9. In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.
10. Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.

* 60-Day *
Policy Review

May 2009

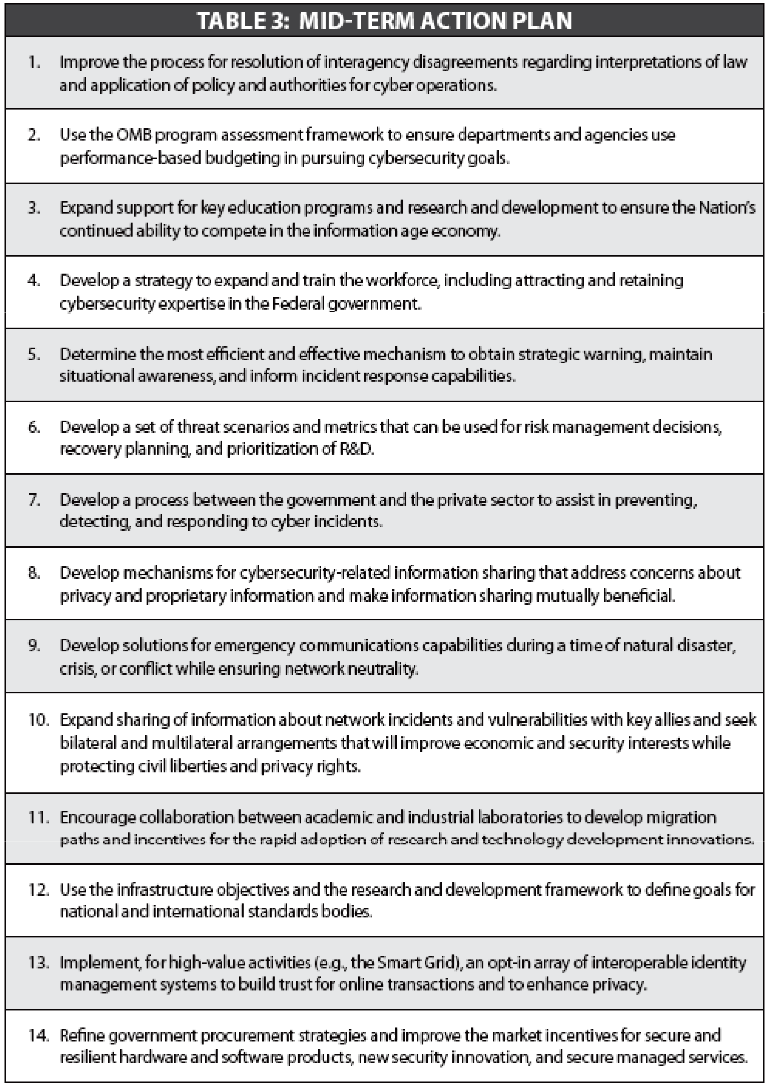
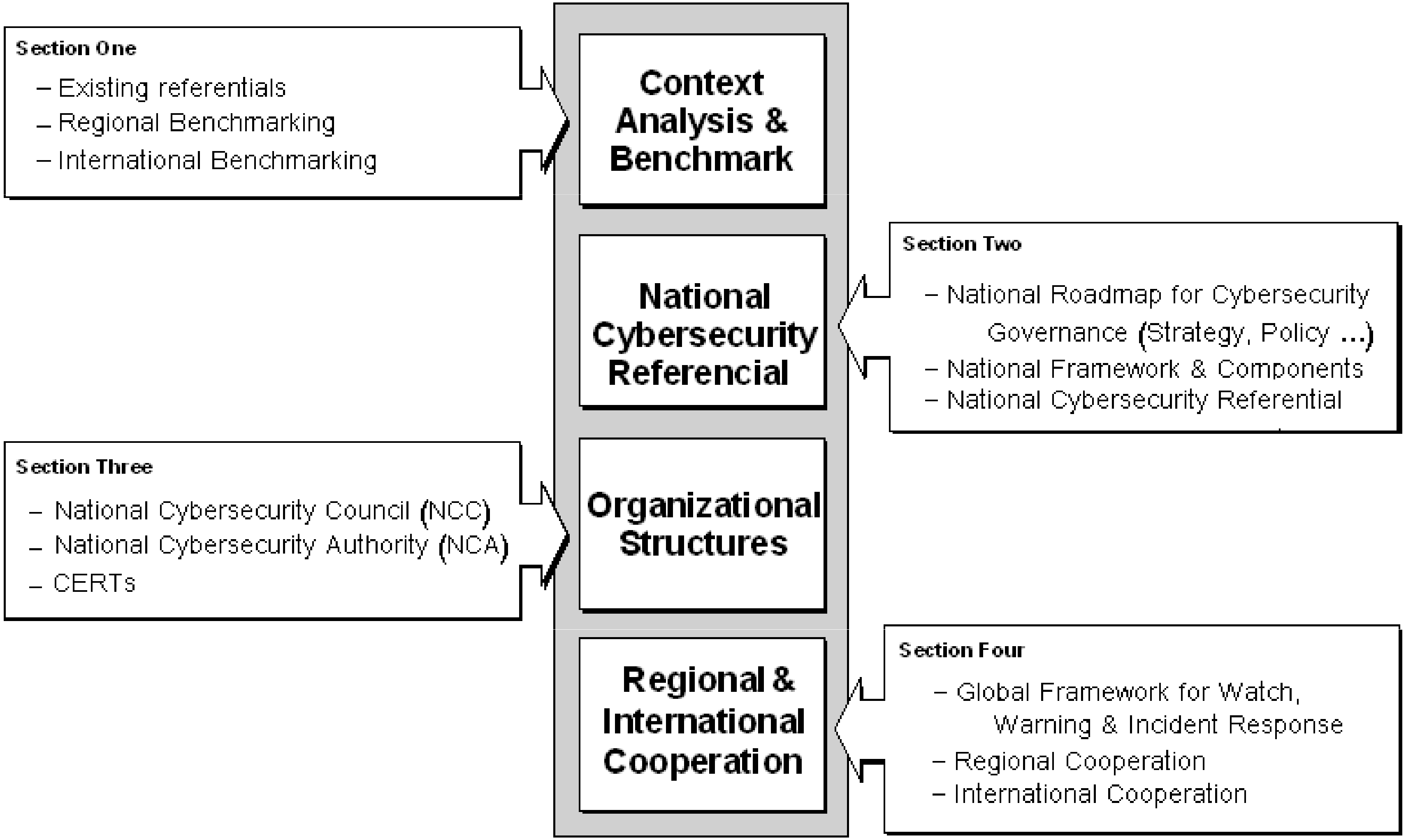


TABLE 3: MID-TERM ACTION PLAN
1. Improve the process for resolution of interagency disagreements regarding interpretations of law and application of policy and authorities for cyber operations.
2. Use the OMB program assessment framework to ensure departments and agencies use performance-based budgeting in pursuing cybersecurity goals.
3. Expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy.
4. Develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the Federal government.
5. Determine the most efficient and effective mechanism to obtain strategic warning, maintain situational awareness, and inform incident response capabilities.
6. Develop a set of threat scenarios and metrics that can be used for risk management decisions, recovery planning, and prioritization of R&D.
7. Develop a process between the government and the private sector to assist in preventing, detecting, and responding to cyber incidents.
8. Develop mechanisms for cybersecurity-related information sharing that address concerns about privacy and proprietary information and make information sharing mutually beneficial.
9. Develop solutions for emergency communications capabilities during a time of natural disaster, crisis, or conflict while ensuring network neutrality.
10. Expand sharing of information about network incidents and vulnerabilities with key allies and seek bilateral and multilateral arrangements that will improve economic and security interests while protecting civil liberties and privacy rights.
11. Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for the rapid adoption of research and technology development innovations.
12. Use the infrastructure objectives and the research and development framework to define goals for national and international standards bodies.
13. Implement, for high-value activities (e.g., the Smart Grid), an opt-in array of interoperable identity management systems to build trust for online transactions and to enhance privacy.
14. Refine government procurement strategies and improve the market incentives for secure and resilient hardware and software products, new security innovation, and secure managed services.

An Approach to Organisational Structures for National Cybersecurity



Section One

- Existing referentials
- Regional Benchmarking
- International Benchmarking

Context Analysis & Benchmark

National Cybersecurity Referencial

Section Two

- National Roadmap for Cybersecurity Governance (Strategy, Policy ...)
- National Framework & Components
- National Cybersecurity Referential

Section Three

- National Cybersecurity Council (NCC)
- National Cybersecurity Authority (NCA)
- CERTs

Organizational Structures

Regional & International Cooperation

Section Four

- Global Framework for Watch, Warning & Incident Response
- Regional Cooperation
- International Cooperation

Structures and Strategies

- *National Cybersecurity Strategy:* The Government Administration first needs to define and communicate its cybersecurity strategy. This strategy will probably be associated with the plans for e-Government

- *National Cybersecurity Agency (NCA):* An effective government agency closely linked to the Cabinet and Ministry of Security is required to co-ordinate resources, and to roll-out the national cybersecurity roadmap

- *Enterprise Organisations:* Businesses will also need to consider the implementation and management of enterprise-wide cybersecurity through the appointment of a Chief Security Officer (CSO) working alongside the Chief Information Officer (CIO)

- *Specialised Cybersecurity Organisations:* There is also a requirement for dedicated organisations such as a national CIRT (Computer Incident Response Team), and National Cybercrime Unit (NCU)

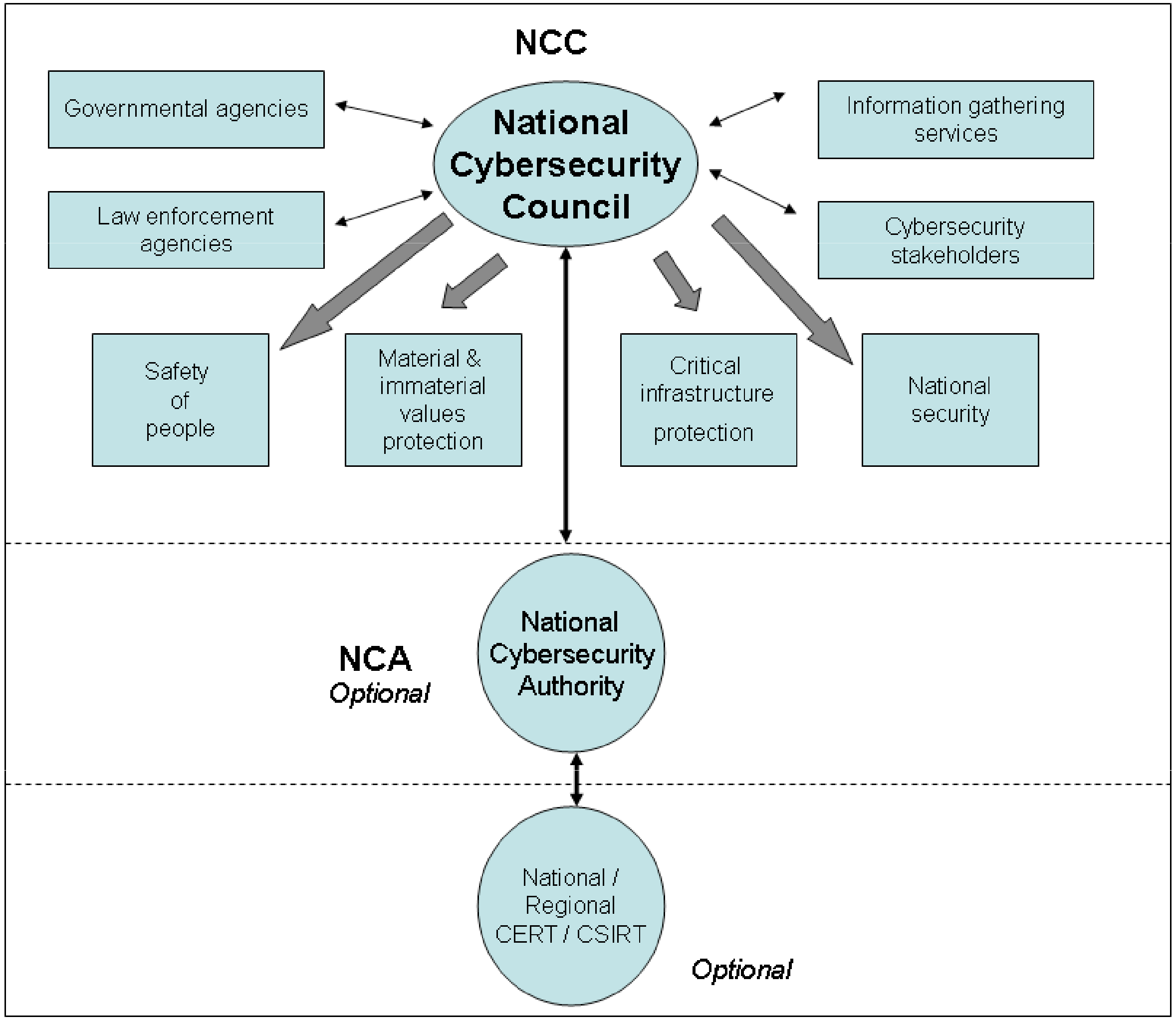
Cybersecurity Co-ordination

- The proposed National Security Agency (or Council) is responsible for the co-ordination of all actions & programmes:

1) Liaison with all the Jamaican Government Ministries & Agencies
2) Co-ordination with Regional & Local Government Organisations
3) Leadership for the Cybersecurity Training and Awareness Programmes
4) Partnerships with Private Business to promote secure eBusiness / eTrade
5) Development and Implementation of Cybercrime Legislation & Regulations
6) Working with the police & military regarding cybercrime / cyberterrorism
7) International Collaboration and Partnerships such as the ITU and Interpol
8) Establish of National CERT/CSIRT for 24/7 National Cyberspace Monitoring
9) Work with Critical Service Sectors such as Banking/Finance, Telecomms, Energy, Education, Healthcare and Travel/Tourism to upgrade cybersecurity

……We'll consider each of these requirements during the course of this session!

Framework for Organisational Structures


NCC
Governmental agencies
National Cybersecurity Council
Information gathering services
Law enforcement agencies
Cybersecurity stakeholders
Safety of people
Material & immaterial values protection
Critical infrastructure protection
National security
NCA
Optional
National Cybersecurity Authority
National / Regional CERT / CSIRT
Optional

National Cyber Agency (NCA)

- We'll briefly consider and summarise the organisation & strategies of the National Cybersecurity Agencies for :

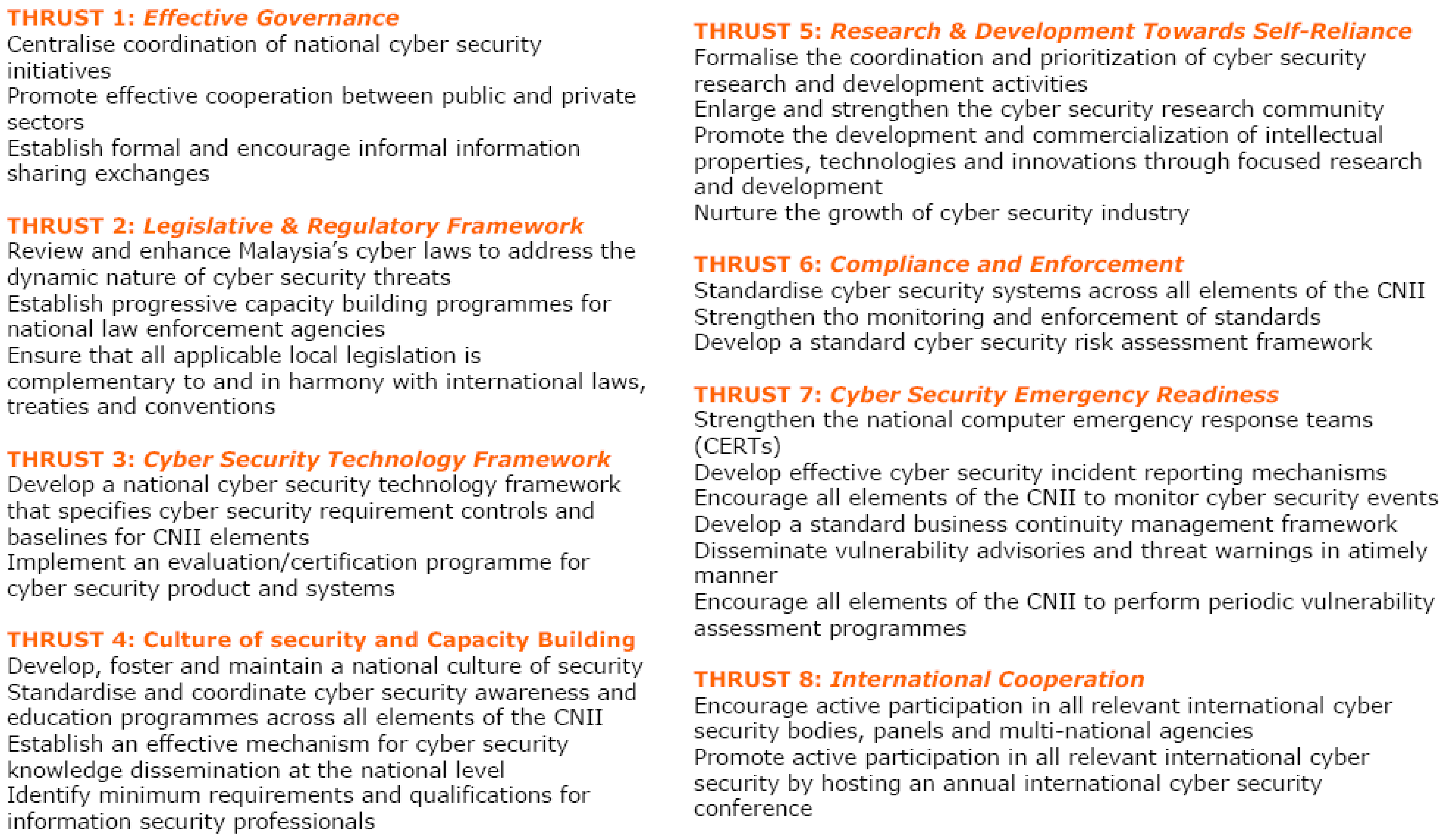
  - *UK Government* - Cybersecurity Strategy for the UK – Safety, Security & Resilience in Cyberspace (UK Office of Cybersecurity – June 2009)
  - *USA Government* - Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure – May 2009
  - *Australian Government* - Australian Cybersecurity Policy and Co-ordination Committee (CSPC – Nov 2009), within Attorney-General's Government Dept
  - *Malaysian Government* - "Cybersecurity Malaysia" – Mosti : Ministry of Science, Technology & Innovation, and includes the MyCERT & Training Centre

… *There are other national agency case studies that we could consider but they all have the common feature that they are driven from the highest level of government and include the 24/7 management of cyber incidents and alerts.*

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

Malaysia: Cybersecurity Strategy

The Eight Policy Thrusts



THRUST 1: *Effective Governance*
Centralise coordination of national cyber security initiatives
Promote effective cooperation between public and private sectors
Establish formal and encourage informal information sharing exchanges

THRUST 2: *Legislative & Regulatory Framework*
Review and enhance Malaysia's cyber laws to address the dynamic nature of cyber security threats
Establish progressive capacity building programmes for national law enforcement agencies
Ensure that all applicable local legislation is complementary to and in harmony with international laws, treaties and conventions

THRUST 3: *Cyber Security Technology Framework*
Develop a national cyber security technology framework that specifies cyber security requirement controls and baselines for CNII elements
Implement an evaluation/certification programme for cyber security product and systems

THRUST 4: Culture of security and Capacity Building
Develop, foster and maintain a national culture of security
Standardise and coordinate cyber security awareness and education programmes across all elements of the CNII
Establish an effective mechanism for cyber security knowledge dissemination at the national level
Identify minimum requirements and qualifications for information security professionals

THRUST 5: *Research & Development Towards Self-Reliance*
Formalise the coordination and prioritization of cyber security research and development activities
Enlarge and strengthen the cyber security research community
Promote the development and commercialization of intellectual properties, technologies and innovations through focused research and development
Nurture the growth of cyber security industry

THRUST 6: *Compliance and Enforcement*
Standardise cyber security systems across all elements of the CNII
Strengthen tho monitoring and enforcement of standards
Develop a standard cyber security risk assessment framework

THRUST 7: *Cyber Security Emergency Readiness*
Strengthen the national computer emergency response teams (CERTs)
Develop effective cyber security incident reporting mechanisms
Encourage all elements of the CNII to monitor cyber security events
Develop a standard business continuity management framework
Disseminate vulnerability advisories and threat warnings in atimely manner
Encourage all elements of the CNII to perform periodic vulnerability assessment programmes

THRUST 8: *International Cooperation*
Encourage active participation in all relevant international cyber security bodies, panels and multi-national agencies
Promote active participation in all relevant international cyber security by hosting an annual international cyber security conference

© Ministry of Science, Technology And Innovation

ITU Cybercrime Toolkit – 2010

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

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

- *Procedural Provisions:* for Criminal Investigations and Proceedings for Offenses Within this Law

- *Jurisdictional Provisions* and International Cooperation

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

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

ITU CYBERCRIME TOOLKIT LEGISLATIVE REQUIREMENTS
Acts Against Computers, Computer Systems, Networks, Computer Data, Content Data, and Traffic Data
Section 1: Definition of Terms
Section 2: Unauthorized Access to Computers, Computer Systems, and Networks
Section 3: Unauthorized Access to or Acquisition of Computer Data, Content Data, Traffic Data
Section 4: Interference and Disruption
Section 5: Interception
Section 6: Misuse and Malware
Section 7: Digital Forgery
Section 8: Digital Fraud, Procure Economic Benefit
Section 9: Extortion
Section 10: Aiding, Abetting, and Attempting
Section 11: Corporate Liability
Provisions for Criminal Investigations and Proceedings for Offenses within this Law
Section 12: Scope of Procedural Provisions
Section 13: Conditions and Safeguards
Section 15: Expedited Preservation and Partial Disclosure of Traffic Data
Section 17: Production Order
Section 18: Search and Seizure of Stored Data
Section 19: Interception (Real Time Collection) of Traffic Data
Section 20: Interception (Real Time Collection) of Content Data

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

Example of National Cybersecurity Action Plan: Short-Term

# Action	SHORT-TERM ACTION PLAN: APRIL – SEPTEMBER 2011
1	**Government Cybersecurity Accountability** Consider making cybersecurity one of the Government’s main management accountabilities with clear success criteria.
2	**Appoint National Cybersecurity Coordinator** Consider designating a senior Government Aide as National Cybersecurity Coordinator. The official should coordinate cybersecurity activities across the Government and report to the appropriate national bodies
3	**Complete and Promulgate National Cybersecurity Strategy** Consider using the template from the ITU Guidelines as a starting point for the National Cybersecurity Strategy. The Strategy should have clear roles and responsibilities, priorities, timeframes and performance metrics. Thereafter, obtain Government approval for the Cybersecurity Strategy.
4	**Create National Cybersecurity Coordination Agency** In common with other countries, consider creating a multi-agency body as a focal point for all activities dealing with protecting ’s cyberspace against threats such as cybercrime.
5	**Define National Cybersecurity Framework** The framework should be flexible to allow stakeholder organisations to achieve the stated goals in the most efficient and effective manner.
6	**Initiate Public-Private Sector Cybersecurity partnership** The process should be transparent and consider all views.
7	**Create Computer Incident Response Team (CIRT)** Consider creating a national CIRT to analyse cyber threat trends, improve response coordination and dissemination of information across the Government, to industry, citizens and international partners.
8	**Strengthen Legal and Regulatory System** Complete the Cybercrime Legislation Programme and enforce the new laws.
9	**Initiate Cybersecurity Awareness and Education campaign** Consider working with the private sector and civil society to explain cyber threats to the citizens and their role in defending cyberspace.
10	**Define and initiate Cybersecurity Skills and Training Programme** Consider the experience of other countries in creating a cybersecurity skills and training programme with periodic measurement of skills.

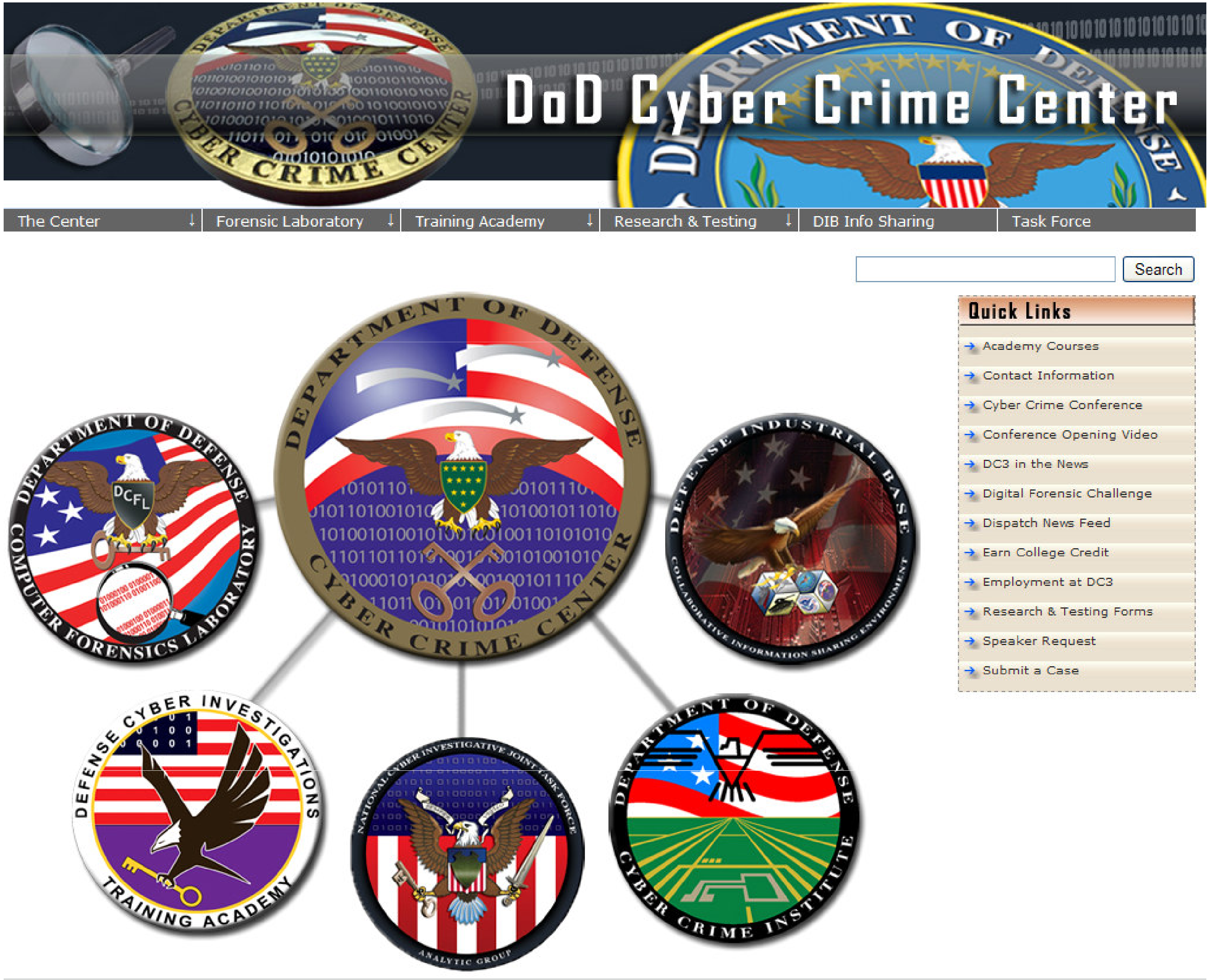
Example of National Cybersecurity Action Plan: Mid-Term

# Action	MID-TERM ACTION PLAN: OCTOBER 2011 – JANUARY 2012
1	Define, localise and communicate Government cybersecurity Standards in areas such as Data Classification and Staff Vetting and Clearance.
2	The National Cybersecurity Agency (NCA) should ensure that cybersecurity policies are in line with the new Cybercrime legislation
3	Launch cybersecurity awareness campaign across Government and NCA website for government, commercial and educational sectors with guidelines, standards and training materials.
4	As National Technical Authority for Information Assurance, the NCA should advise on how to secure eGovernment Services.
5	Use formal channels to organise study trips for NCA Staff to other Cybersecurity Agencies
6	Conduct in-depth cybersecurity review and audit of Government ministries, agencies and associated bodies.
7	Review Physical Security of organisations hosting critical infrastructure.
8	Parliamentary review of the proposed National Cybersecurity Act 2011
9	NCA Programme on Business Continuity and Disaster Recovery
10	Develop and Resource the national CIRT/CERT. In addition, develop national Cyber Incident Response Framework involving public-private stakeholders. Also develop, test and exercise incident response plans for Government emergency communications during natural disasters, cyberattacks, crisis or war as required by the National Security Concept.
11	Implement six to nine months' programme of Operational Cybersecurity upgrades. The activities may extend into 2011 and beyond.
12	Ensure that the Government Communications Network and all new services comply with the agreed Government Authentication Framework.
13	Launch the Cybersecurity Skills and Training Programme for cybersecurity professionals and collaborate with commercial and educational sectors to boost cybersecurity Research and Development.
14	Secure Parliamentary, Cabinet & Government approval of the Cybersecurity Act 2011 and associated Cybercrime legislation.
15	Organise an annual Regional Cybersecurity Conference to communicate progress, share views and promote national Cybersecurity Programme.

Cybersecurity Organisational Structures & Incident Management for CITEL-OAS

1 –Aim: National Cybersecurity	2 – Critical Service Sectors	3 – Cyber Attack Scenarios
4–"Best Practice" Case Studies	5–CERT: Organisational Models	6 – The "Cyber" Business Case
7 – Global IMPACT Alliance	8 - Public-Private Partnership	9 – Next Suggested Steps

US Government – Cyber Crime Center


DoD Cyber Crime Center
The Center
Forensic Laboratory
Training Academy
Research & Testing
DIB Info Sharing
Task Force
Search
DEPARTMENT OF DEFENSE CYBER CRIME CENTER
DEPARTMENT OF DEFENSE COMPUTER FORENSICS LABORATORY
DCFL
DEFENSE INDUSTRIAL BASE COLLABORATIVE INFORMATION SHARING ENVIRONMENT
DEFENSE CYBER INVESTIGATIONS TRAINING ACADEMY
NATIONAL CYBER INVESTIGATIVE JOINT TASK FORCE ANALYTICAL GROUP
DEPARTMENT OF DEFENSE CYBER CRIME INSTITUTE

Quick Links

- Academy Courses
- Contact Information
- Cyber Crime Conference
- Conference Opening Video
- DC3 in the News
- Digital Forensic Challenge
- Dispatch News Feed
- Earn College Credit
- Employment at DC3
- Research & Testing Forms
- Speaker Request
- Submit a Case

Emergency and Security Incident Response – CERTs/CIRTs/CSIRTs -

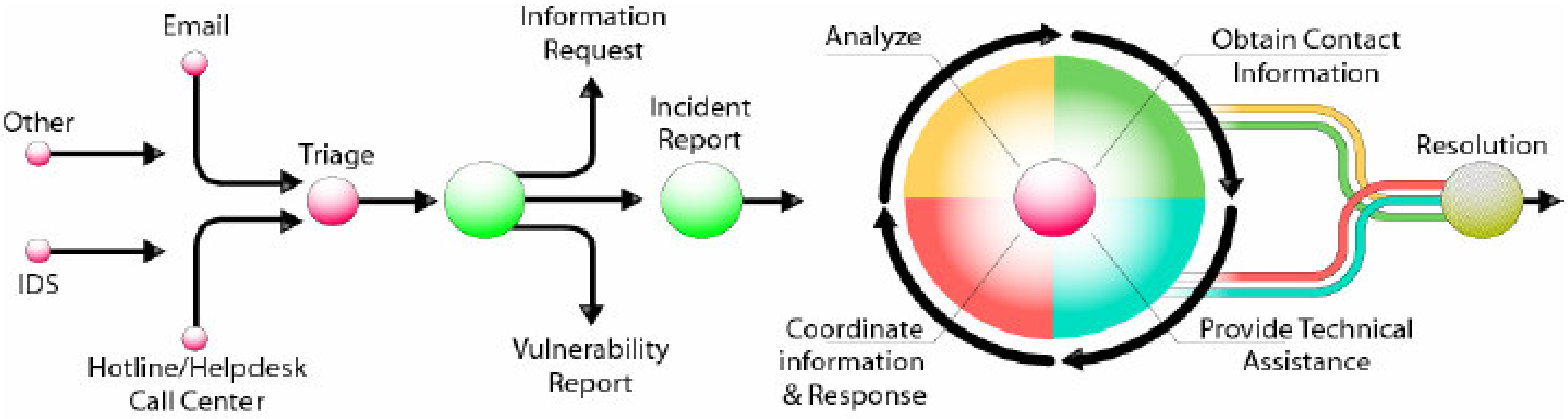
- The provision of a CERT (Computer Emergency Response Team) , CIRT (Computer Incident Response Team) or CSIRT will be a top priority for any new National or Sector-based Cybersecurity Organisation. In many countries the “Education Sector” will already have built some form of CERT/CIRT/CSIRT for their own needs.

- There are many excellent on-line guides to the establishment of a CERT/CIRT/CSIRT such as “Organizational Models for CSIRTs”-Published by Carnegie Mellon University. Many such useful documents can be downloaded from www.cert.org & www.first.org

- The European Agency – ENISA – is another excellent source for the latest research and guides to the installation and management of national CERTs/CSIRTs

- Practically all the operational CERTs are members of a much wider international CERT community that shares information regarding the latest cyber incidents, alerts, malicious attacks & hackers. They will often work together to identify the source of international cyberattacks, and hence to counter major cyberthreats

Incident Handling Life-Cycle


Email
Other
IDS
Hotline/Helpdesk Call Center
Triage
Information Request
Incident Report
Vulnerability Report
Analyze
Obtain Contact Information
Resolution
Coordinate information & Response
Provide Technical Assistance

CIRT – Information Process Flow

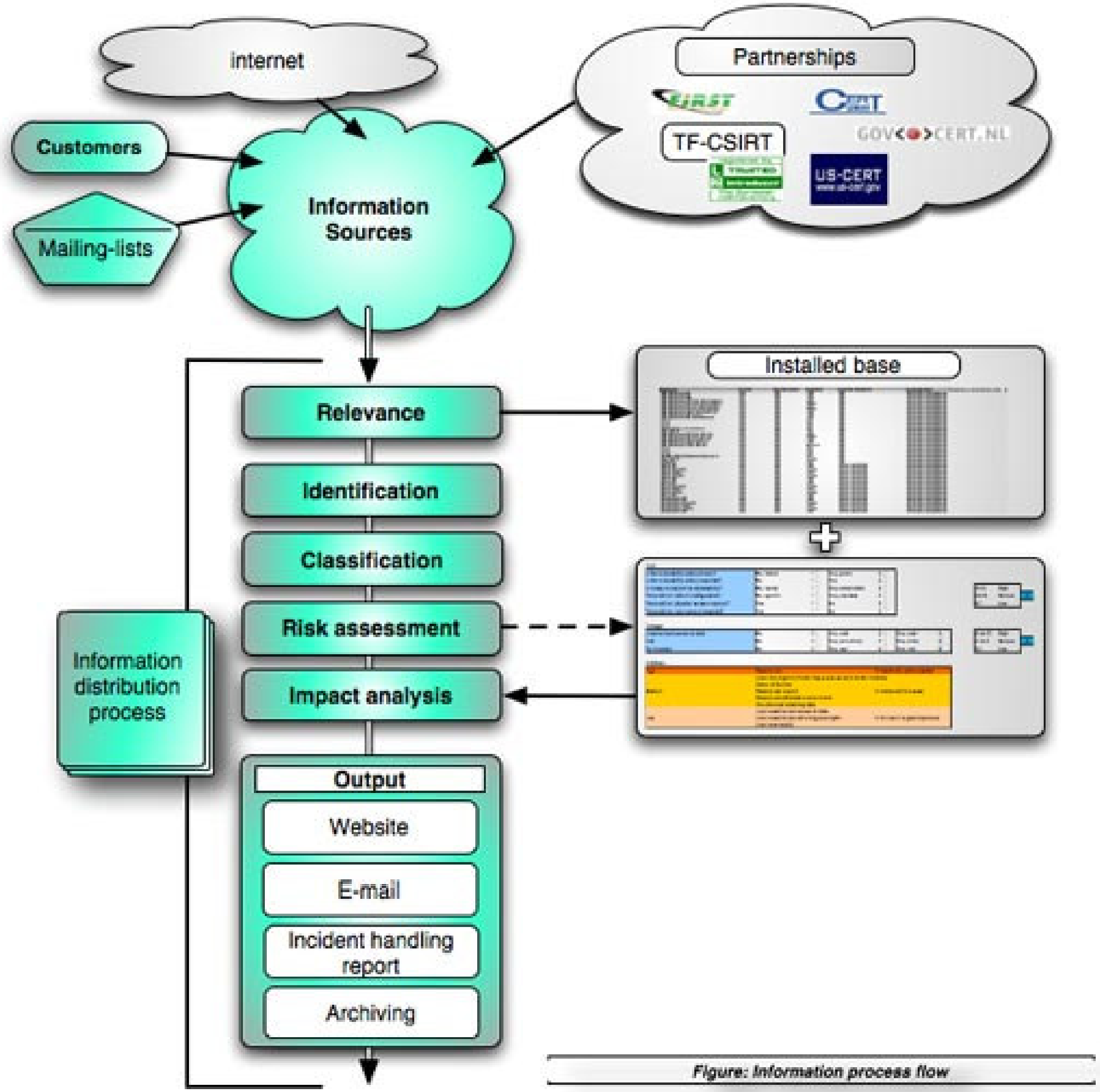


Figure: Information process flow

Incident Handling Process Flow

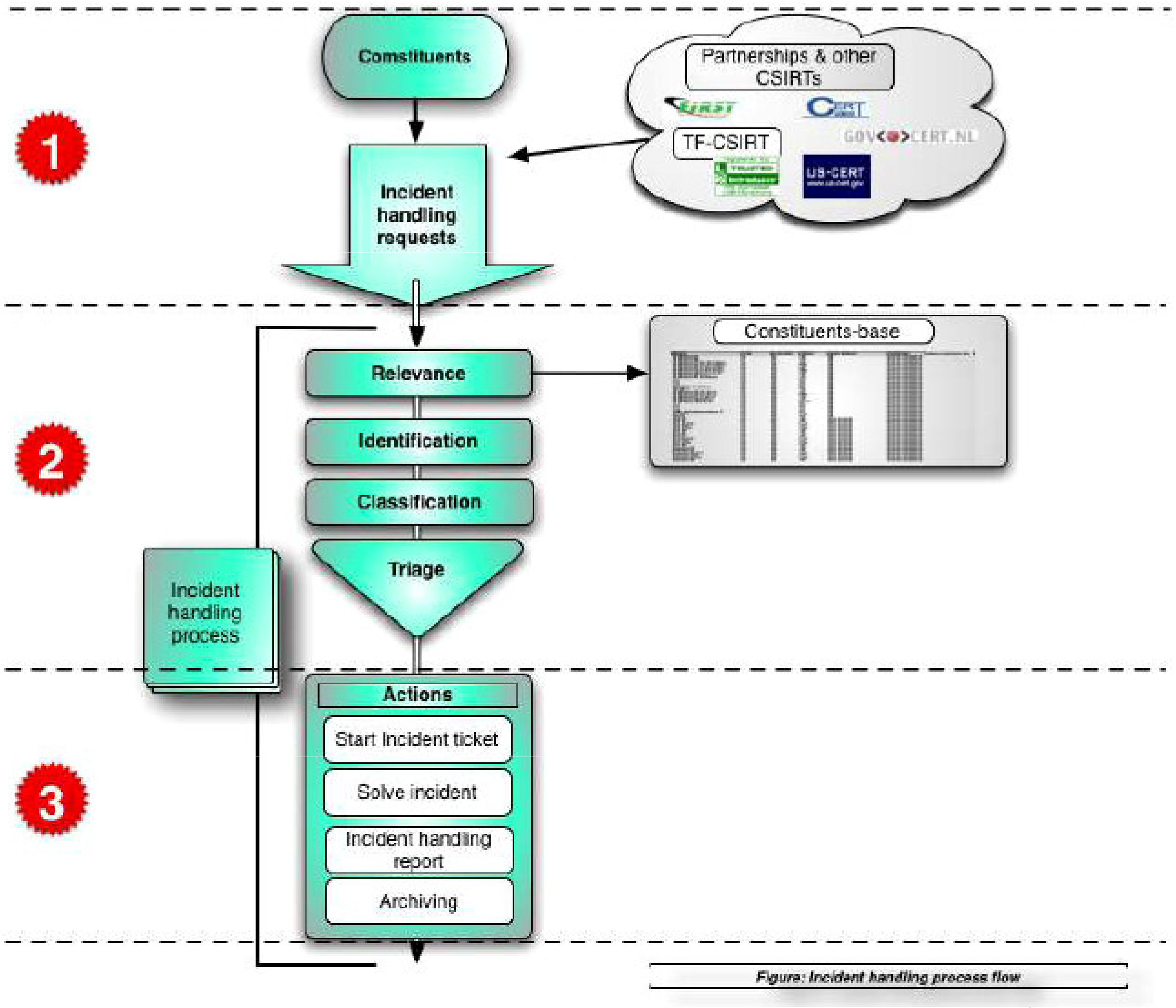
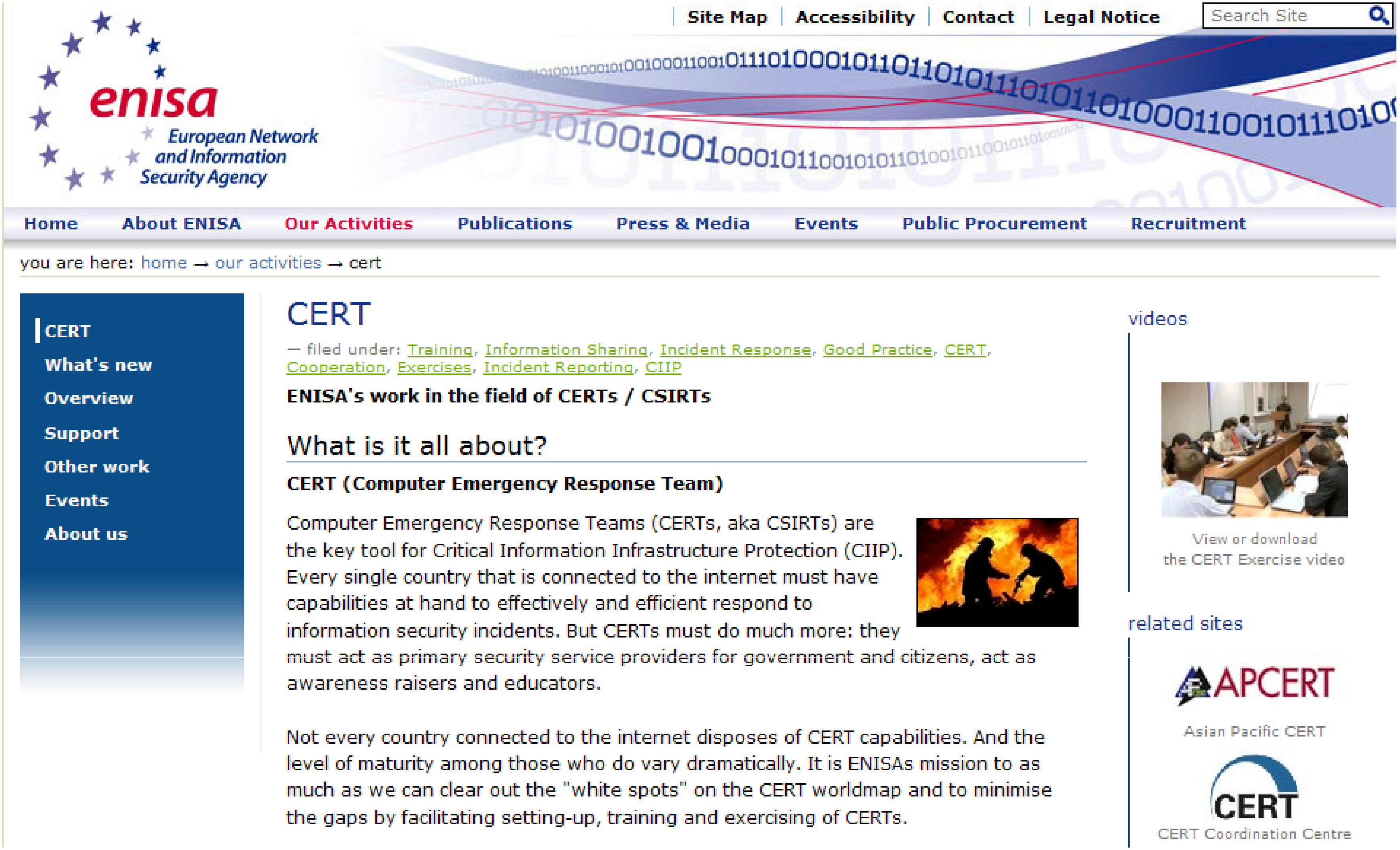


Figure: Incident handling process flow

European Union : ENISA



enisa
European Network and Information Security Agency
Site Map | Accessibility | Contact | Legal Notice
Search Site
Home About ENISA Our Activities Publications Press & Media Events Public Procurement Recruitment
CERT
What's new
Overview
Support
Other work
Events
About us
videos
related sites

you are here: home → our activities → cert

CERT

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

ENISA's work in the field of CERTs / CSIRTs

What is it all about?

CERT (Computer Emergency Response Team)

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

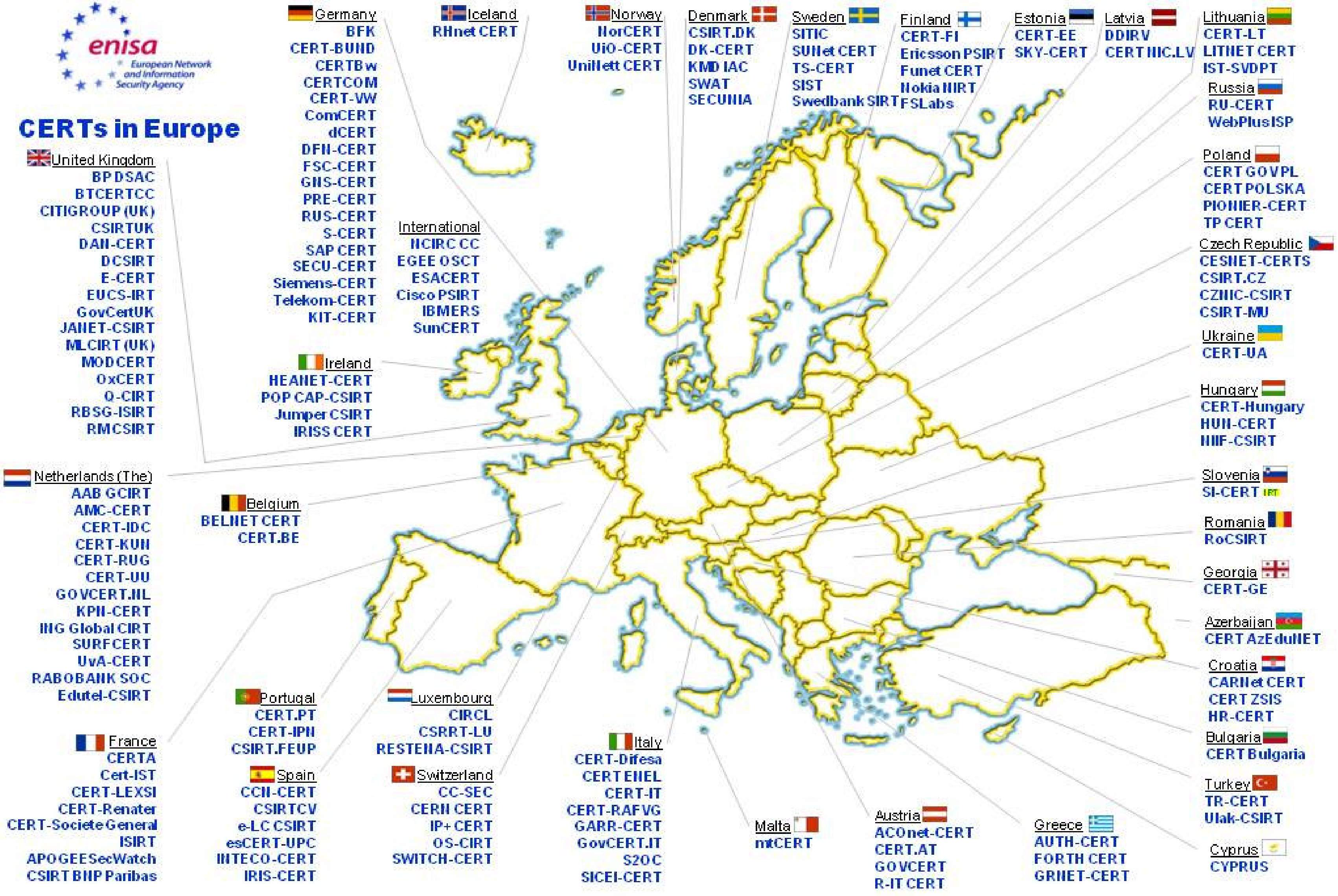
Not every country connected to the internet disposes of CERT capabilities. And the level of maturity among those who do vary dramatically. It is ENISAs mission to as much as we can clear out the "white spots" on the CERT worldmap and to minimise the gaps by facilitating setting-up, training and exercising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

View or download the CERT Exercise video

APCERT
Asian Pacific CERT

CERT
CERT Coordination Centre

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

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

Iceland
RHnet CERT

International
NCIRC CC
EGEE OSCT
ESACERT
Cisco PSIRT
IBMERS
SunCERT

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

Norway
NorCERT
UiO-CERT
UniNett CERT

Denmark
CSIRT.DK
DK-CERT
KMD IAC
SWAT
SECUNIA

Sweden
SITIC
SUNet CERT
TS-CERT
SIST
Swedbank SIRT

Finland
CERT-FI
Ericsson PSIRT
Funet CERT
Nokia NIRT
FSLabs

Estonia
CERT-EE
SKY-CERT

Latvia
DDIRV
CERT NIC.LV

Lithuania
CERT-LT
LITNET CERT
IST-SVDPT

Russia
RU-CERT
WebPlus ISP

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

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

Belgium
BELNET CERT
CERT.BE

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

Portugal
CERT.PT
CERT-IPN
CSIRT.FEUP

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

Luxembourg
CIRCL
CSRRT-LU
RESTENA-CSIRT

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

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

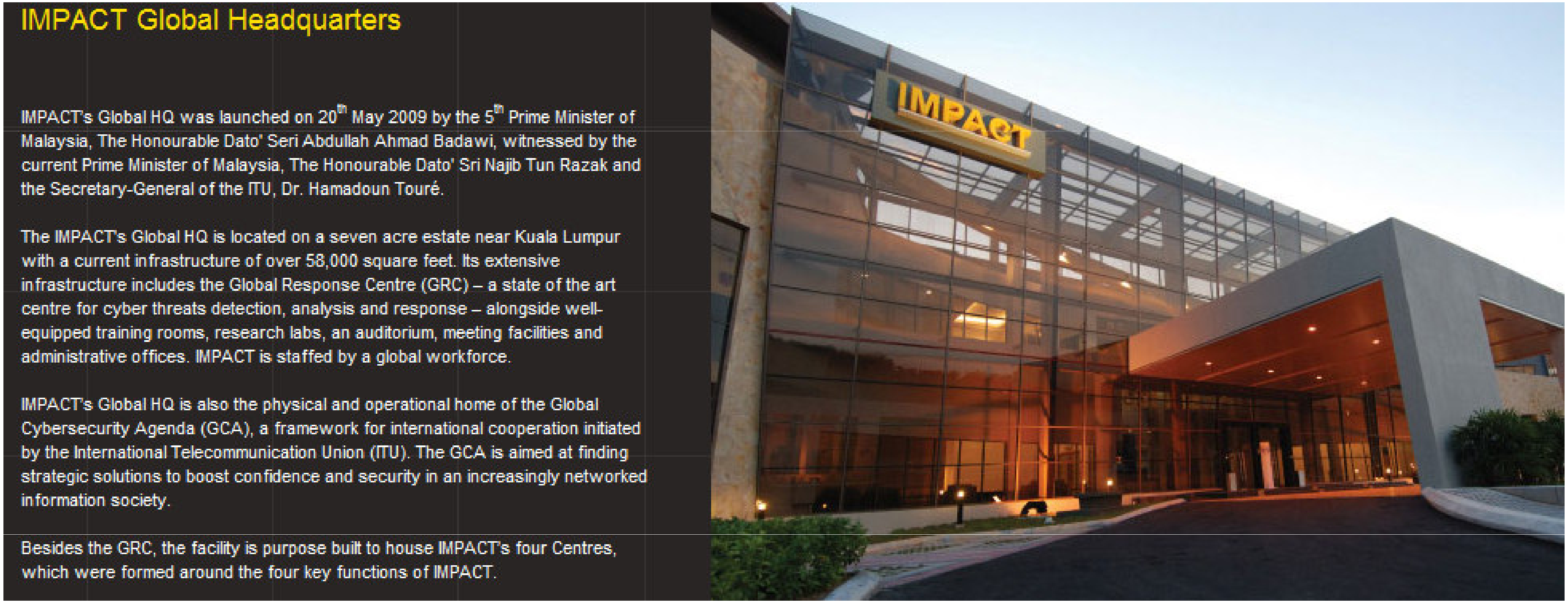
Malta
mtCERT

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

Greece
AUTH-CERT
FORTH CERT
GRNET-CERT

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

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.

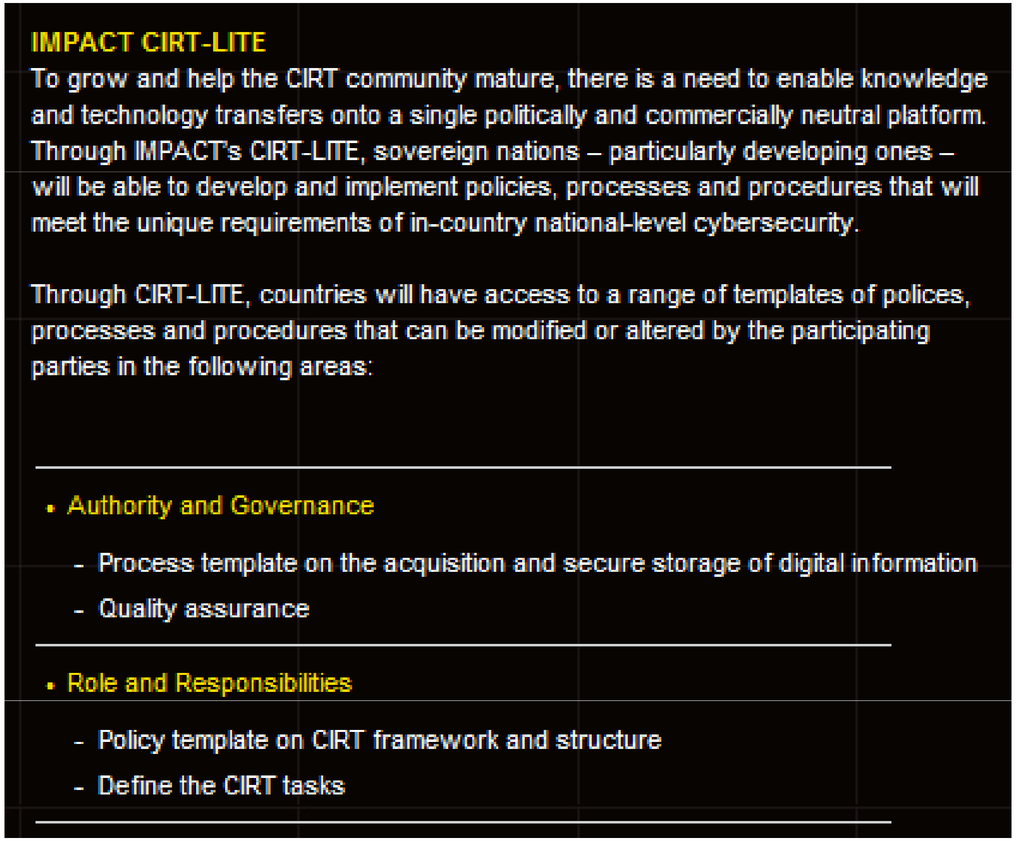
The IMPACT's Global HQ is located on a seven acre estate near Kuala Lumpur with a current infrastructure of over 58,000 square feet. Its extensive infrastructure includes the Global Response Centre (GRC) – a state of the art centre for cyber threats detection, analysis and response – alongside well-equipped 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

ITU-IMPACT: CIRT-LITE Programme

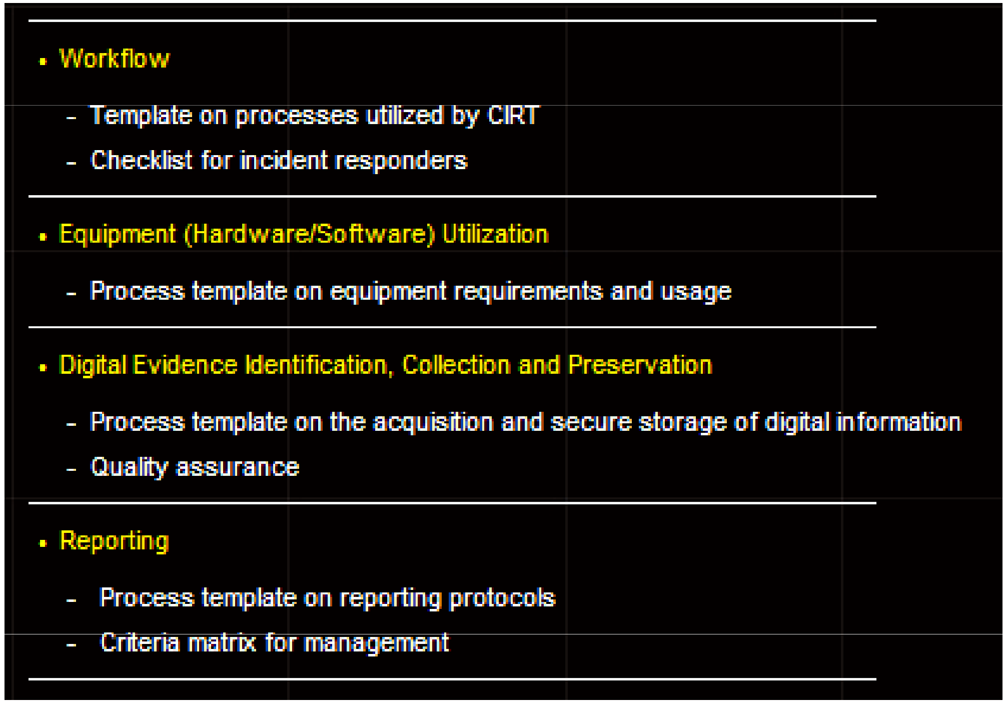


IMPACT CIRT-LITE

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

ITU : IMPACT Programme (B)

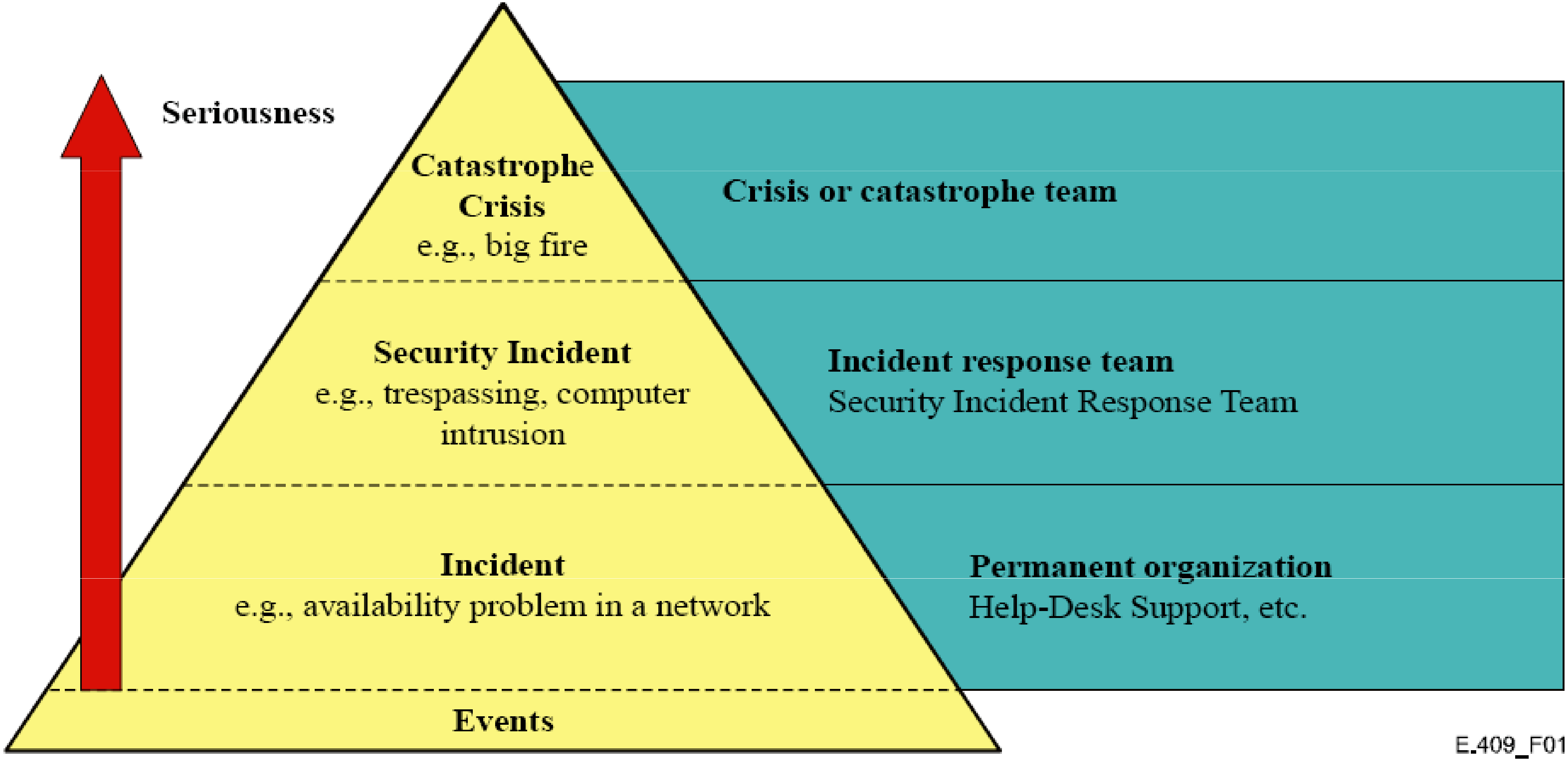
- *IMPACT* is an outstanding example of the 1st New Generation 21stCentury Worldwide *PPP* Organisation that is dedicated to the challenge of tackling global Cyberthreats, Cybercrimes, Cyberattacks and Cyberterrorism

- *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 the CIRT-LITE Service

- 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

Pyramid of Critical Events – ITU: E409



Seriousness

Catastrophe
Crisis
e.g., big fire

Crisis or catastrophe team

Security Incident
e.g., trespassing, computer intrusion

Incident response team
Security Incident Response Team

Incident
e.g., availability problem in a network

Permanent organization
Help-Desk Support, etc.

Events

E.409_F01