Overview of ITU-D Activities Related to Cybersecurity and Critical Information Infrastructure Protection

ITU Regional Workshop on Frameworks for Cybersecurity and CIIP
Doha, Qatar
18-21 February 2008

Robert Shaw
Head, ICT Applications and Cybersecurity Division
Policies and Strategies Department
ITU Telecommunication Development Sector

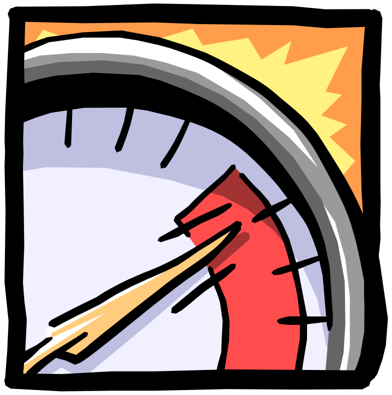
Introduction to ITU

- International organization where governments and private sector coordinate global telecom networks and services
- Founded in 1865, it is oldest specialized agency of the UN system
- 191 Member States, 780 Sector Members & Sector Associates
- Headquarters Geneva, 11 regional offices, 760 staff / 80 nationalities

ITU Mission & More

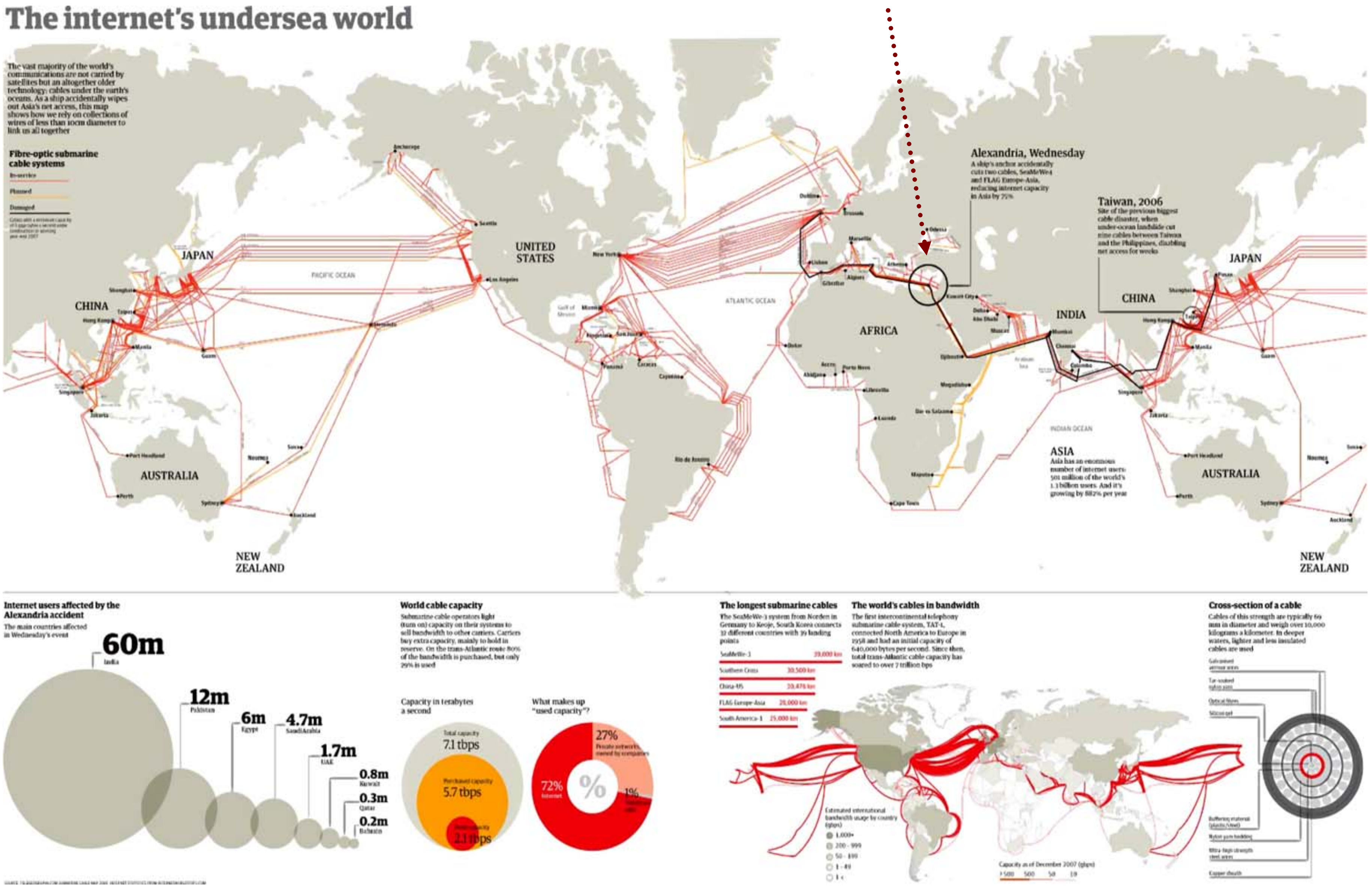
- Maintain and extend international cooperation in telecommunications
- Technical and policy assistance to developing countries
- To harmonize actions of Member States and promote cooperation between Member States and Sector Members
- Instigator and manager of the World Summit on the Information Society (WSIS) held in two phases
- ITU named as one of the world's ten most enduring institutions by US university scholars

Setting the Context



- In the 21st century, growing dependency on information and communications technologies (ICTs) that span the globe;
- Rapid growth in ICTs and dependencies led to shift in perception of cybersecurity threats in mid-1990s;
- Growing linkage of cybersecurity and critical information infrastructure protection (CIIP);
- Number of countries began assessment of threats, vulnerabilities and explored mechanisms to redress them;
- But most countries have not formulated or implemented a national strategy for cybersecurity or CIIP;
- In parallel with national consideration, move to international political agenda.

Is Cybersecurity/CIIP Important?
Net Outage – February 2008



The internet's undersea world

The vast majority of the world's communications are not carried by satellites but an altogether older technology: cables under the earth's oceans. As a ship accidentally wipes out Asia's net access, this map shows how we rely on collections of wires of less than 10cm diameter to link us all together

Fibre-optic submarine cable systems

In-service

Planned

Damaged

Alexandria, Wednesday

A ship's anchor accidentally cuts two cables, SeaMeWe4 and FLAG Europe-Asia, reducing internet capacity in Asia by 75%

Taiwan, 2006

Site of the previous biggest cable disaster, when under-ocean landslide cut nine cables between Taiwan and the Philippines, disabling net access for weeks

ASIA

Asia has an enormous number of internet users: 501 million of the world's 1.1 billion users. And it's growing by 882% per year

Internet users affected by the Alexandria accident

The main countries affected in Wednesday's event

World cable capacity

Submarine cable operators light (turn on) capacity on their systems to sell bandwidth to other carriers. Carriers buy extra capacity, mainly to hold in reserve. On the trans-Atlantic route 80% of the bandwidth is purchased, but only 29% is used

The longest submarine cables

The SeaMeWe-3 system from Norden in Germany to Keoje, South Korea connects 32 different countries with 39 landing points

SeaMeWe-3	39,000 km
Southern Cross	30,500 km
China-US	30,476 km
FLAG Europe-Asia	28,000 km
South America-1	25,000 km

The world's cables in bandwidth

The first intercontinental telephony submarine cable system, TAT-1, connected North America to Europe in 1958 and had an initial capacity of 640,000 bytes per second. Since then, total trans-Atlantic cable capacity has soared to over 7 trillion bps

Cross-section of a cable

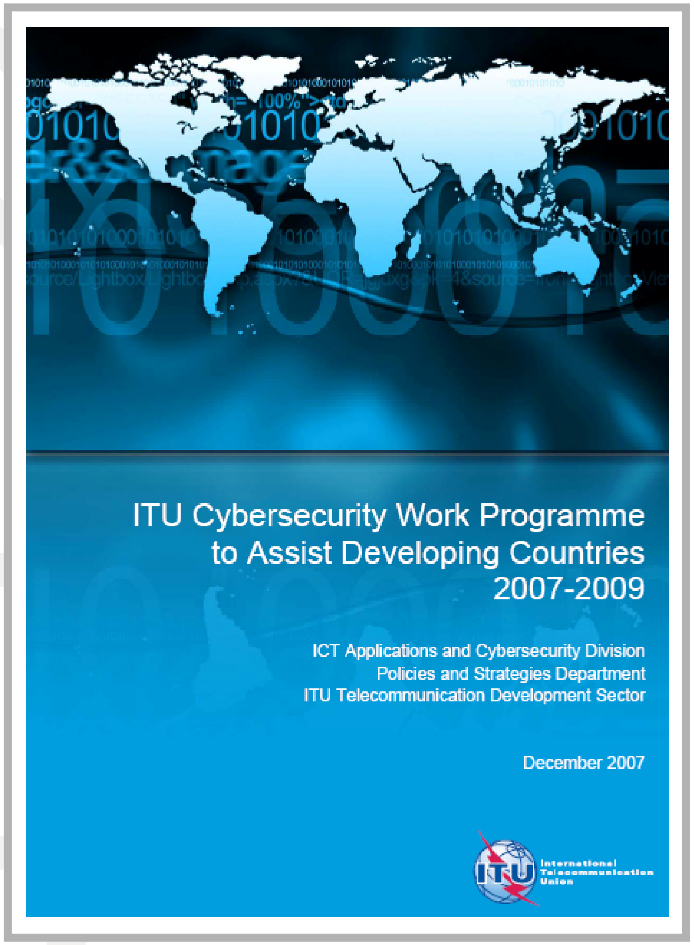
Cables of this strength are typically 69 mm in diameter and weigh over 10,000 kilograms a kilometer. In deeper waters, lighter and less insulated cables are used

ITU Development Sector Role

- From ITU Plenipotentiary Conference (Antalya, 2006):
  - Resolution 130: Strengthening the role of ITU in building confidence and security in the use of information and communication technologies;
- From World Telecommunication Development Conference (Doha, 2006):
  - ITU-D Study Group 1 Question 22/1
  - Cybersecurity part of *Programme 3* managed by *ITU-D ICT Applications and Cybersecurity Division*

Key Activities Underway

- ITU-D Study Group 1 Question 22/1: *Securing information and communication networks: Best practices for developing a culture of cybersecurity*
  - Developing *Framework for Organizing a National Approach to Cybersecurity*
- ITU-D Programme 3 *ITU Cybersecurity Work Programme to Assist Developing Countries*
- Close synergies between these two activities



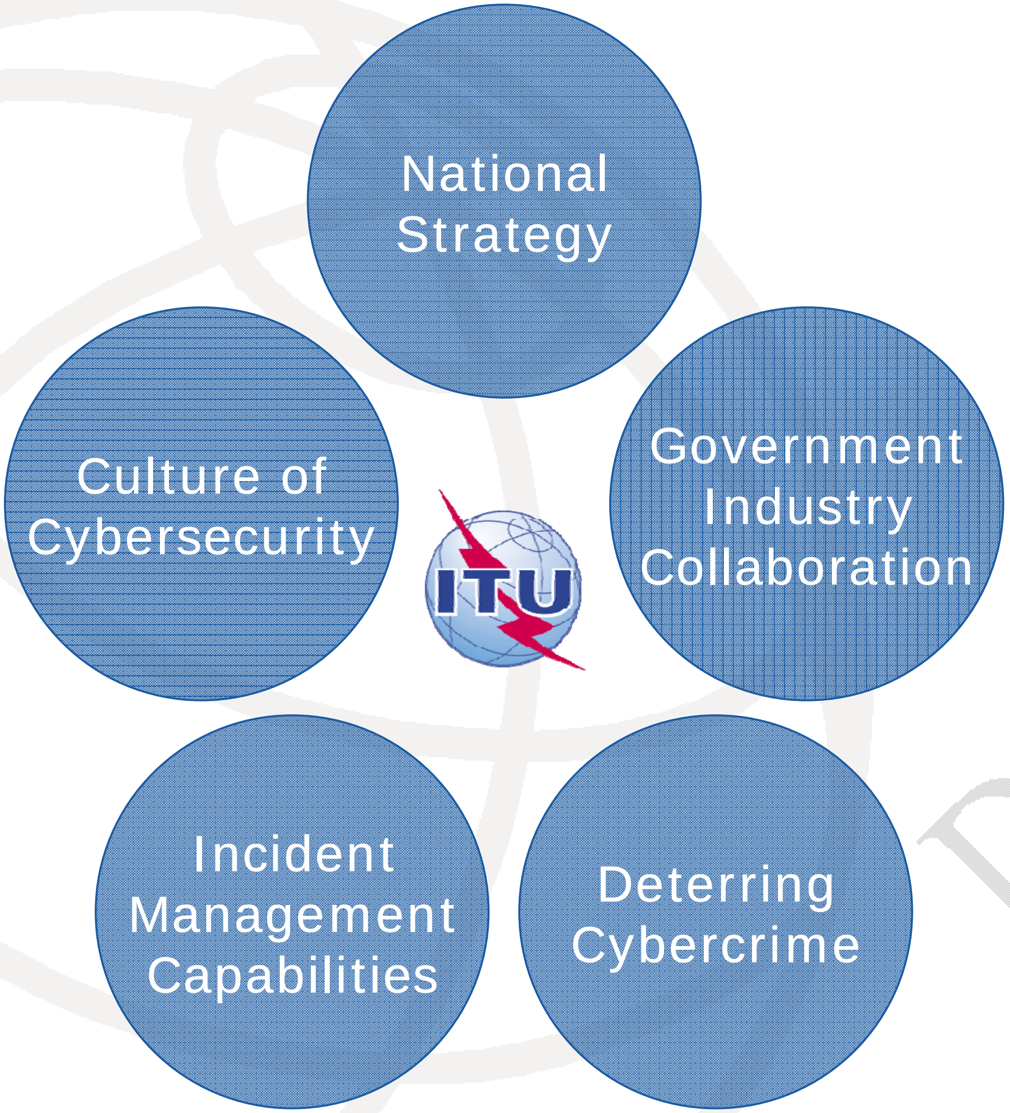
ITU Cybersecurity Work Programme
to Assist Developing Countries
2007-2009

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

December 2007

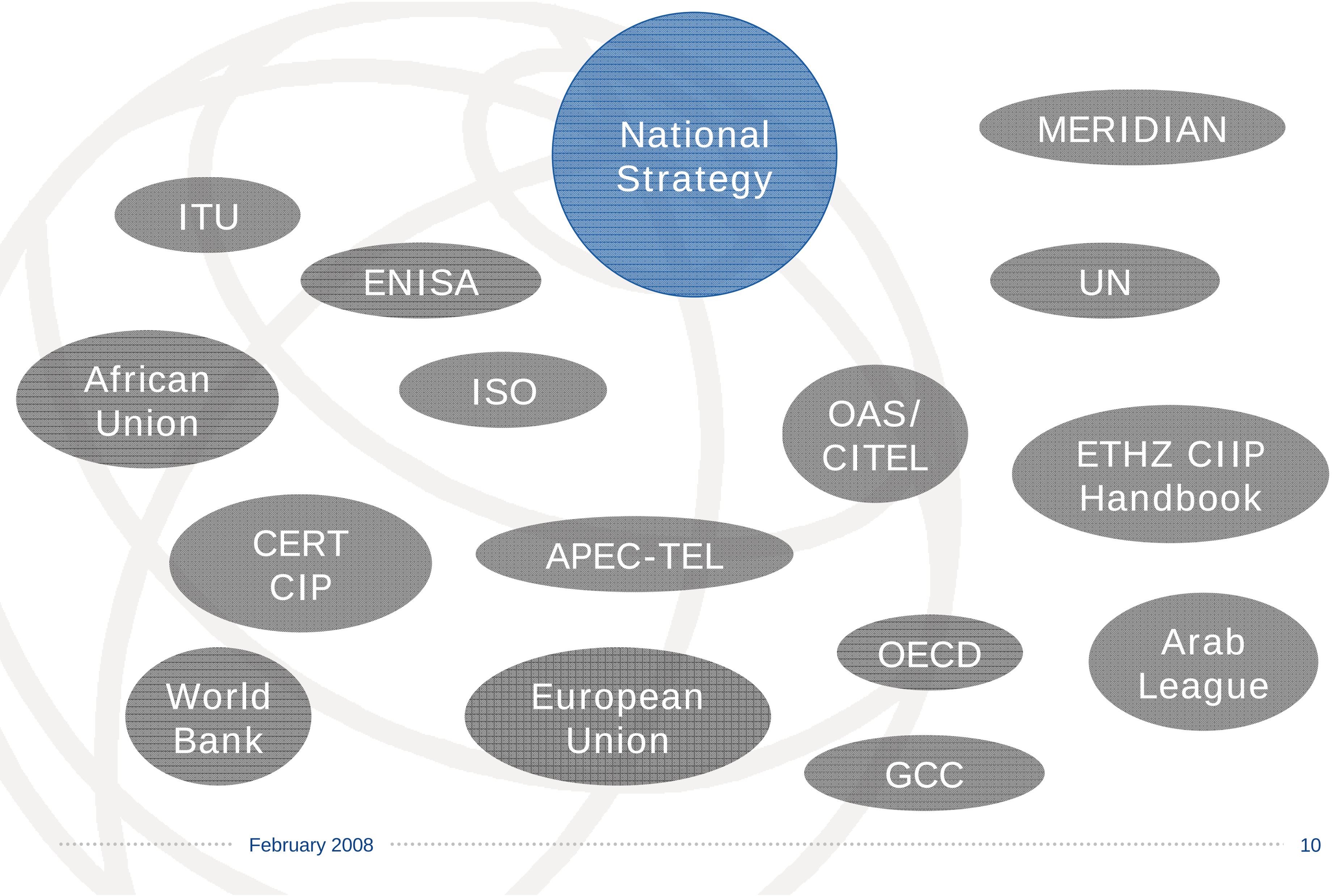
International Telecommunication Union

ITU Cybersecurity Framework

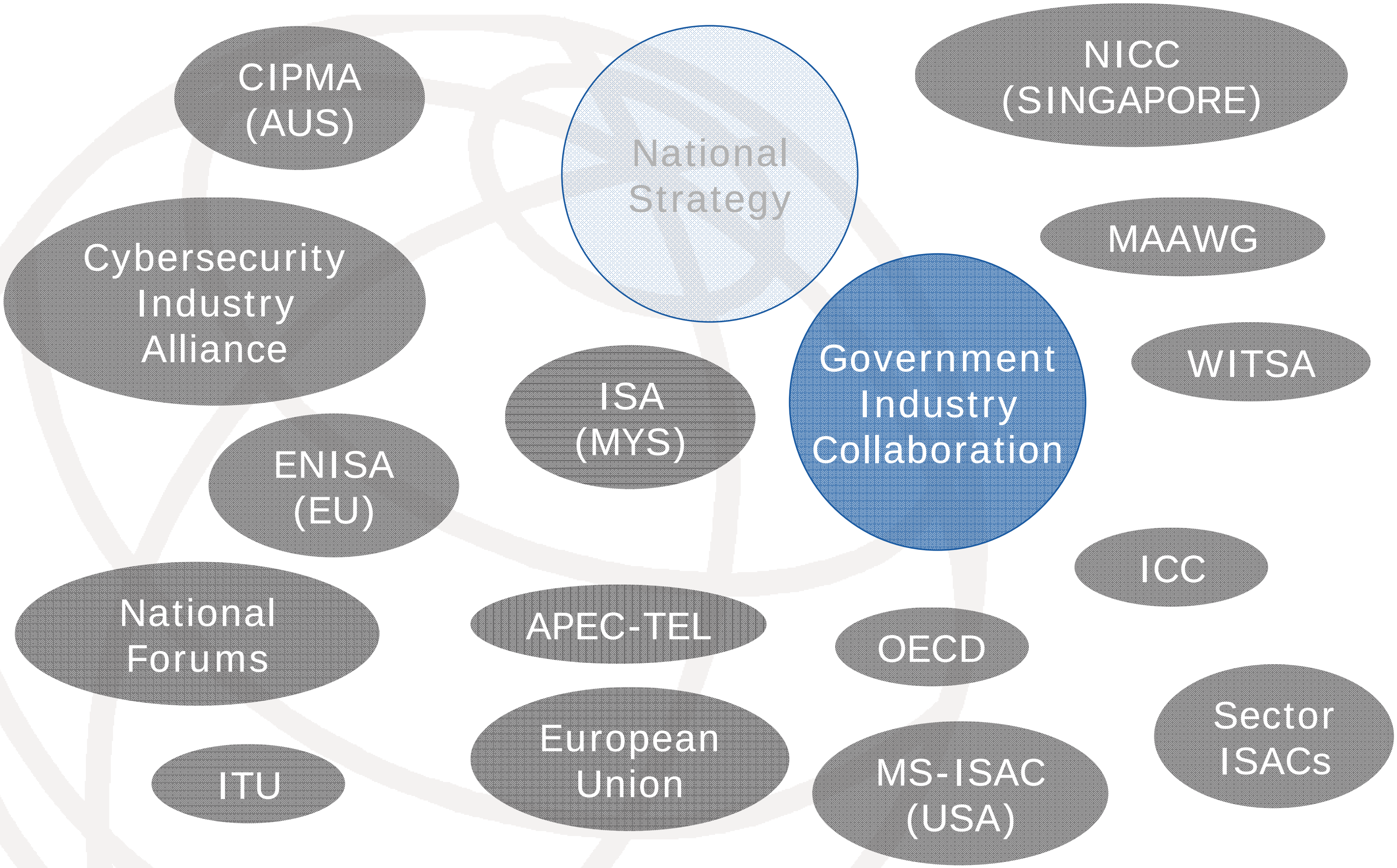

National Strategy
Culture of Cybersecurity
Government Industry Collaboration
ITU
Incident Management Capabilities
Deterring Cybercrime

Thousands of Existing Initiatives and Actors Involved

ITU Cybersecurity Framework



ITU Cybersecurity Framework



CIPMA (AUS)

National Strategy

NICC (SINGAPORE)

Cybersecurity Industry Alliance

MAAWG

Government Industry Collaboration

WITSA

ISA (MYS)

ENISA (EU)

ICC

National Forums

APEC-TEL

OECD

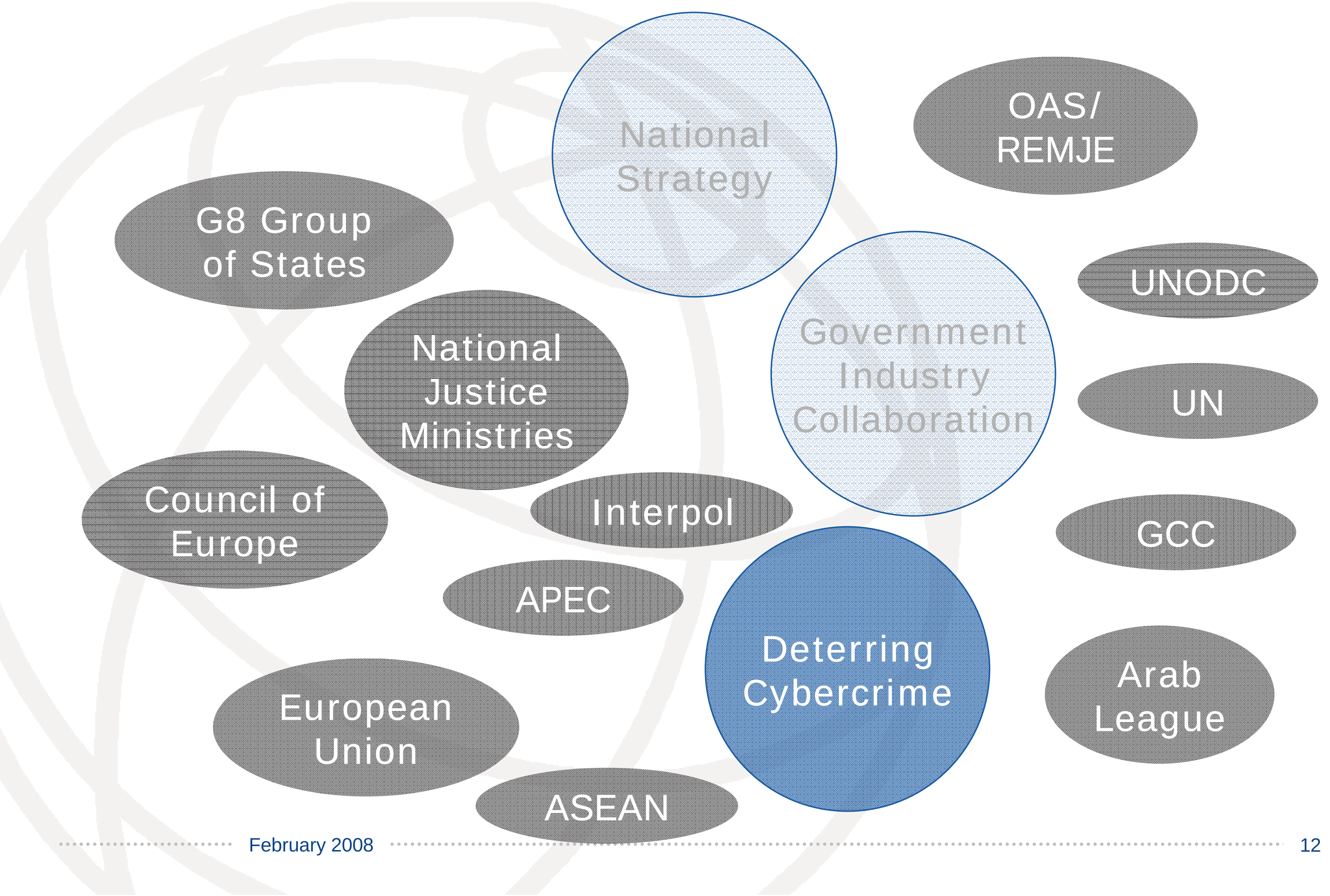
Sector ISACs

ITU

European Union

MS-ISAC (USA)

ITU Cybersecurity Framework



National Strategy

OAS/ REMJE

G8 Group of States

Government Industry Collaboration

UNODC

National Justice Ministries

UN

Council of Europe

Interpol

GCC

APEC

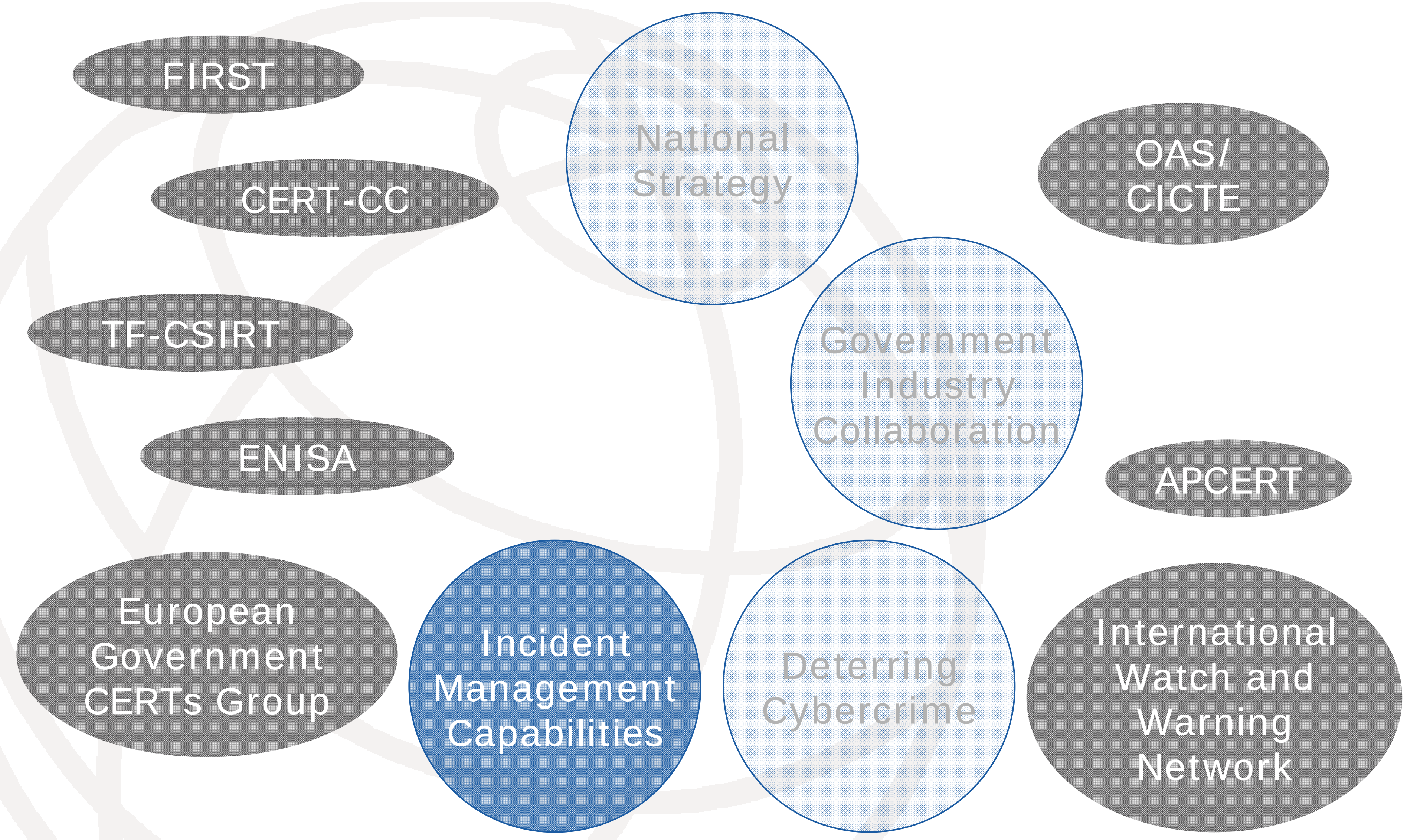
Deterring Cybercrime

Arab League

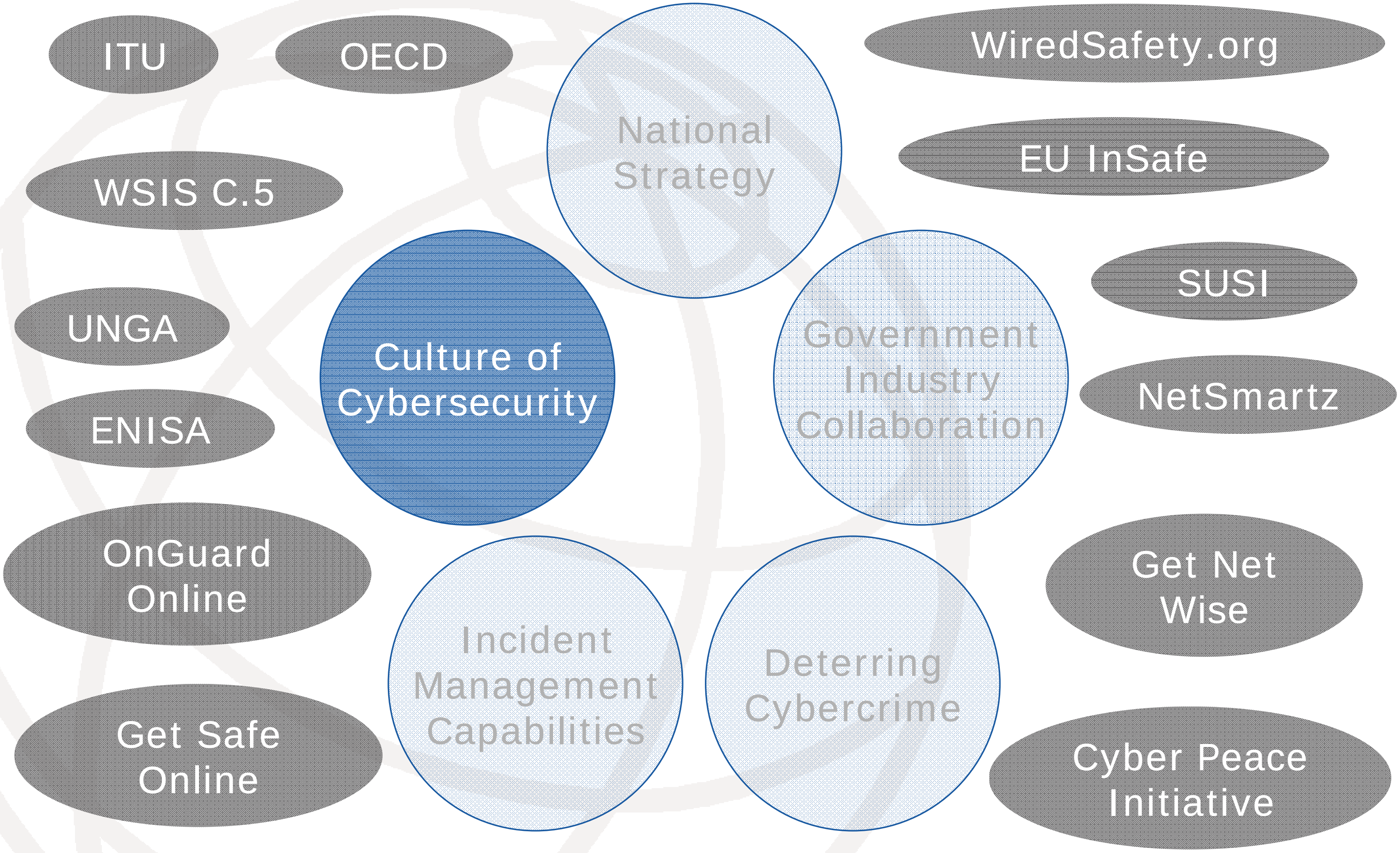
European Union

ASEAN

ITU Cybersecurity Framework


FIRST
CERT-CC
TF-CSIRT
ENISA
European Government CERTs Group
National Strategy
Government Industry Collaboration
Incident Management Capabilities
Deterring Cybercrime
OAS/ CICTE
APCERT
International Watch and Warning Network

ITU Cybersecurity Framework



ITU

OECD

WSIS C.5

UNGA

ENISA

OnGuard Online

Get Safe Online

National Strategy

Culture of Cybersecurity

Government Industry Collaboration

Incident Management Capabilities

Deterring Cybercrime

WiredSafety.org

EU InSafe

SUSI

NetSmartz

Get Net Wise

Cyber Peace Initiative

ITU Efforts to Support Framework and National Implementation Efforts

- Reference material and training resources
- Toolkits including ITU National Cybersecurity/CIIP Self-Assessment Toolkit
- Regional Cybersecurity Forums
  - August 2007: Vietnam
  - October 2007: Argentina
  - November 2007: Cape Verde
  - February 2008: Qatar
  - June 2008: Australia
  - August 2008: Zambia (TBC)
  - October 2008: Bulgaria
  - November 2008: Tunisia

Cybersecurity Work Programme to Assist Developing Countries: High Level Elements

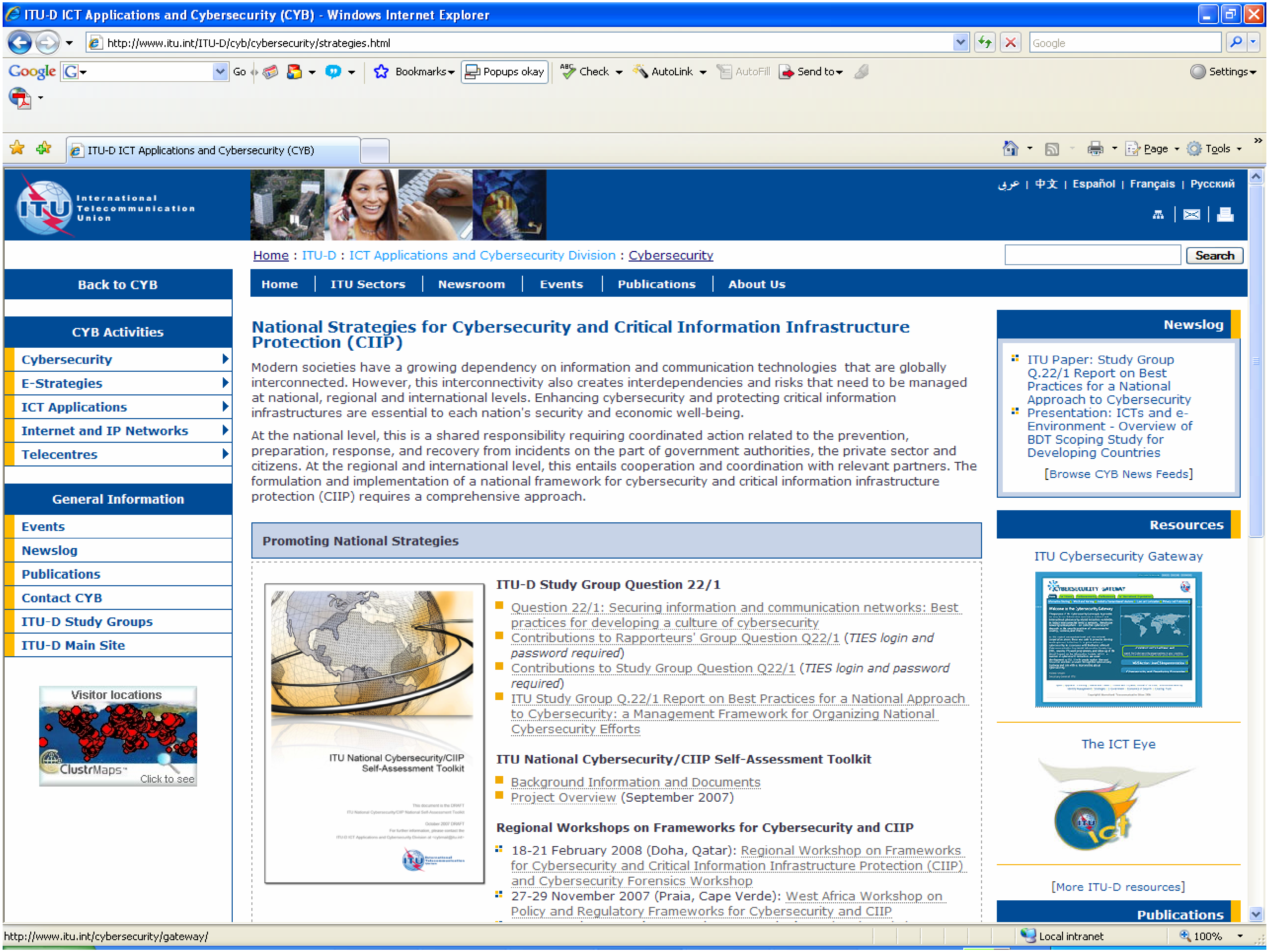
- Assistance related to Establishment of National Strategies and Capabilities for Cybersecurity and Critical Information Infrastructure Protection (CIIP)
- Assistance related to Establishment of appropriate Cybercrime Legislation and Enforcement Mechanisms
- Assistance related to establishment of Watch, Warning and Incident Response (WWIR) Capabilities
- Assistance related to Countering Spam and Related Threats
- Assistance in Bridging Security-Related Standardization Gap between Developing and Developed Countries
- Establishment of an ITU Cybersecurity/CIIP Directory, Contact Database and Who's Who Publication
- Cybersecurity Indicators
- Fostering Regional Cooperation Activities
- Information Sharing and Supporting the ITU Cybersecurity Gateway
- Outreach and Promotion of Related Activities

www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf

Specific Activities: Some Examples

National Strategies/Capabilities for Cybersecurity & CIIP

- Establishment of National Frameworks for Cybersecurity & CIIP
- National Cybersecurity/CIIP Readiness Self-Assessment Toolkit
  - Pilot tests in selected countries
- Regional Cybersecurity Forums on Frameworks for Cybersecurity and CIIP
- Online Experts Forum to Help Developing Countries Develop Capacity
- Toolkit for Promoting a Culture of Cybersecurity (2008)
- Online Training Modules for Cybersecurity Awareness and Solutions
- References:
  - http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
  - http://www.itu.int/ITU-D/cyb/cybersecurity/strategies.html
  - http://www.itu.int/ITU-D/cyb/events/


ITU-D ICT Applications and Cybersecurity (CYB) - Windows Internet Explorer
http://www.itu.int/ITU-D/cyb/cybersecurity/strategies.html
Google
Go
Bookmarks
Popups okay
Check
AutoLink
AutoFill
Send to
Settings
ITU-D ICT Applications and Cybersecurity (CYB)
Page
Tools
International Telecommunication Union
عربي | 中文 | Español | Français | Русский
Search
http://www.itu.int/cybersecurity/gateway/
Local intranet
100%

Home : ITU-D : ICT Applications and Cybersecurity Division : Cybersecurity

Home | ITU Sectors | Newsroom | Events | Publications | About Us

Back to CYB

CYB Activities

- Cybersecurity
- E-Strategies
- ICT Applications
- Internet and IP Networks
- Telecentres

General Information

- Events
- Newslog
- Publications
- Contact CYB
- ITU-D Study Groups
- ITU-D Main Site

Visitor locations

ClustrMaps™ Click to see

National Strategies for Cybersecurity and Critical Information Infrastructure Protection (CIIP)

Modern societies have a growing dependency on information and communication technologies that are globally interconnected. However, this interconnectivity also creates interdependencies and risks that need to be managed at national, regional and international levels. Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security and economic well-being.

At the national level, this is a shared responsibility requiring coordinated action related to the prevention, preparation, response, and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and international level, this entails cooperation and coordination with relevant partners. The formulation and implementation of a national framework for cybersecurity and critical information infrastructure protection (CIIP) requires a comprehensive approach.

Promoting National Strategies

ITU National Cybersecurity/CIIP Self-Assessment Toolkit

ITU-D Study Group Question 22/1

- Question 22/1: Securing information and communication networks: Best practices for developing a culture of cybersecurity
- Contributions to Rapporteurs' Group Question Q22/1 (*TIES login and password required*)
- Contributions to Study Group Question Q22/1 (*TIES login and password required*)
- ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: a Management Framework for Organizing National Cybersecurity Efforts

ITU National Cybersecurity/CIIP Self-Assessment Toolkit

- Background Information and Documents
- Project Overview (September 2007)

Regional Workshops on Frameworks for Cybersecurity and CIIP

- 18-21 February 2008 (Doha, Qatar): Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP) and Cybersecurity Forensics Workshop
- 27-29 November 2007 (Praia, Cape Verde): West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP

Newslog

- ITU Paper: Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity
- Presentation: ICTs and e-Environment - Overview of BDT Scoping Study for Developing Countries

[Browse CYB News Feeds]

Resources

ITU Cybersecurity Gateway

The ICT Eye

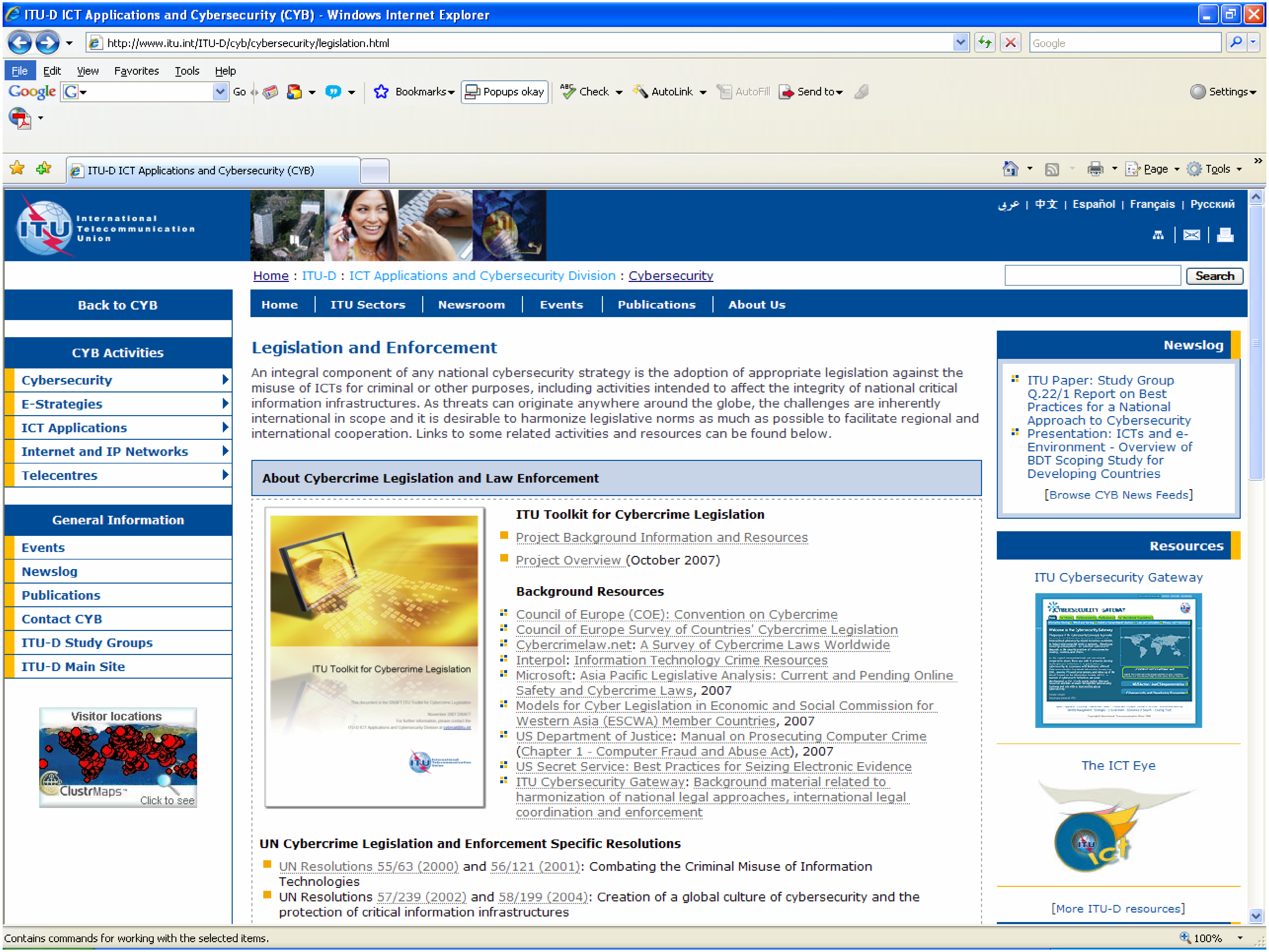
[More ITU-D resources]

Publications

Establishment of Appropriate Cybercrime Legislation and Enforcement Mechanisms

- Regional Capacity Building Activities on Cybercrime Legislation and Enforcement
- Cybercrime Publication: undergoing editing, published in early 2008
- ITU Toolkit for Cybercrime Legislation (2008)

- References
  - www.itu.int/ITU-D/cyb/cybersecurity/legislation.html


ITU-D ICT Applications and Cybersecurity (CYB) - Windows Internet Explorer
http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html
Google
File Edit View Favorites Tools Help
Go Bookmarks Popups okay Check AutoLink AutoFill Send to Settings
ITU-D ICT Applications and Cybersecurity (CYB)
Page Tools
International Telecommunication Union
عربي | 中文 | Español | Français | Русский
Search
Contains commands for working with the selected items.
100%

[Home](#) : ITU-D : ICT Applications and Cybersecurity Division : [Cybersecurity](#)

Home | ITU Sectors | Newsroom | Events | Publications | About Us

Back to CYB

CYB Activities

- Cybersecurity
- E-Strategies
- ICT Applications
- Internet and IP Networks
- Telecentres

General Information

- Events
- Newslog
- Publications
- Contact CYB
- ITU-D Study Groups
- ITU-D Main Site

Visitor locations

ClustrMaps™ Click to see

Legislation and Enforcement

An integral component of any national cybersecurity strategy is the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures. As threats can originate anywhere around the globe, the challenges are inherently international in scope and it is desirable to harmonize legislative norms as much as possible to facilitate regional and international cooperation. Links to some related activities and resources can be found below.

About Cybercrime Legislation and Law Enforcement

ITU Toolkit for Cybercrime Legislation

ITU Toolkit for Cybercrime Legislation

- Project Background Information and Resources
- Project Overview (October 2007)

Background Resources

- Council of Europe (COE): Convention on Cybercrime
- Council of Europe Survey of Countries' Cybercrime Legislation
- Cybercrimelaw.net: A Survey of Cybercrime Laws Worldwide
- Interpol: Information Technology Crime Resources
- Microsoft: Asia Pacific Legislative Analysis: Current and Pending Online Safety and Cybercrime Laws, 2007
- Models for Cyber Legislation in Economic and Social Commission for Western Asia (ESCWA) Member Countries, 2007
- US Department of Justice: Manual on Prosecuting Computer Crime (Chapter 1 - Computer Fraud and Abuse Act), 2007
- US Secret Service: Best Practices for Seizing Electronic Evidence
- ITU Cybersecurity Gateway: Background material related to harmonization of national legal approaches, international legal coordination and enforcement

UN Cybercrime Legislation and Enforcement Specific Resolutions

- UN Resolutions 55/63 (2000) and 56/121 (2001): Combating the Criminal Misuse of Information Technologies
- UN Resolutions 57/239 (2002) and 58/199 (2004): Creation of a global culture of cybersecurity and the protection of critical information infrastructures

Newslog

- ITU Paper: Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity
- Presentation: ICTs and e-Environment - Overview of BDT Scoping Study for Developing Countries

[Browse CYB News Feeds]

Resources

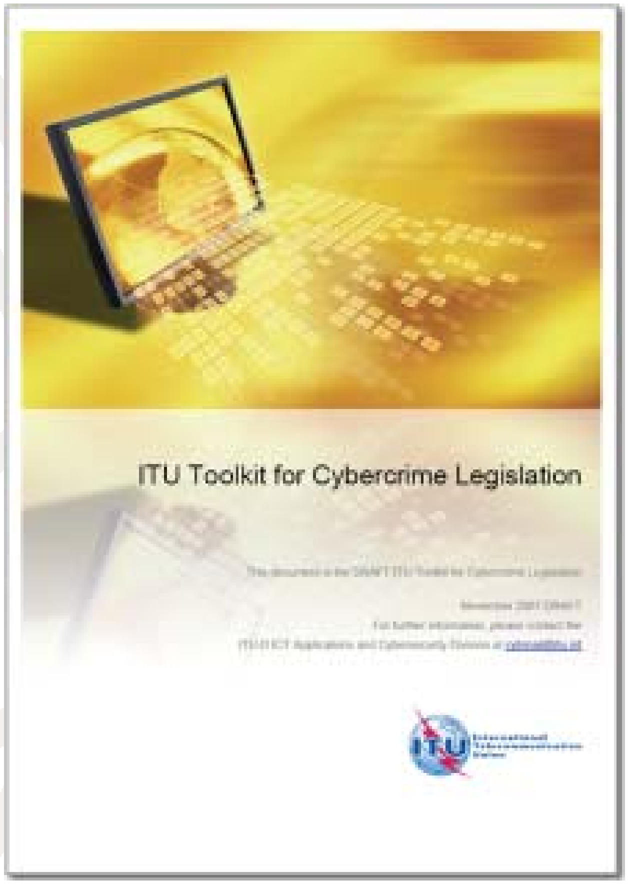
ITU Cybersecurity Gateway

The ICT Eye

[More ITU-D resources]

ITU Toolkit for Cybercrime Legislation

- Representing one of five elements Q22/1, deterring cybercrime is an integral component of a national cybersecurity/CIIP strategy
- ITU Toolkit for Cybercrime Legislation aims to provide countries with reference material that can assist in the establishment of a legislative framework to deter cybercrime;
- Development of toolkit undertaken by multidisciplinary international group of experts:
  - first draft early 2008.


ITU Toolkit for Cybercrime Legislation

This document is the DRAFT ITU Toolkit for Cybercrime Legislation

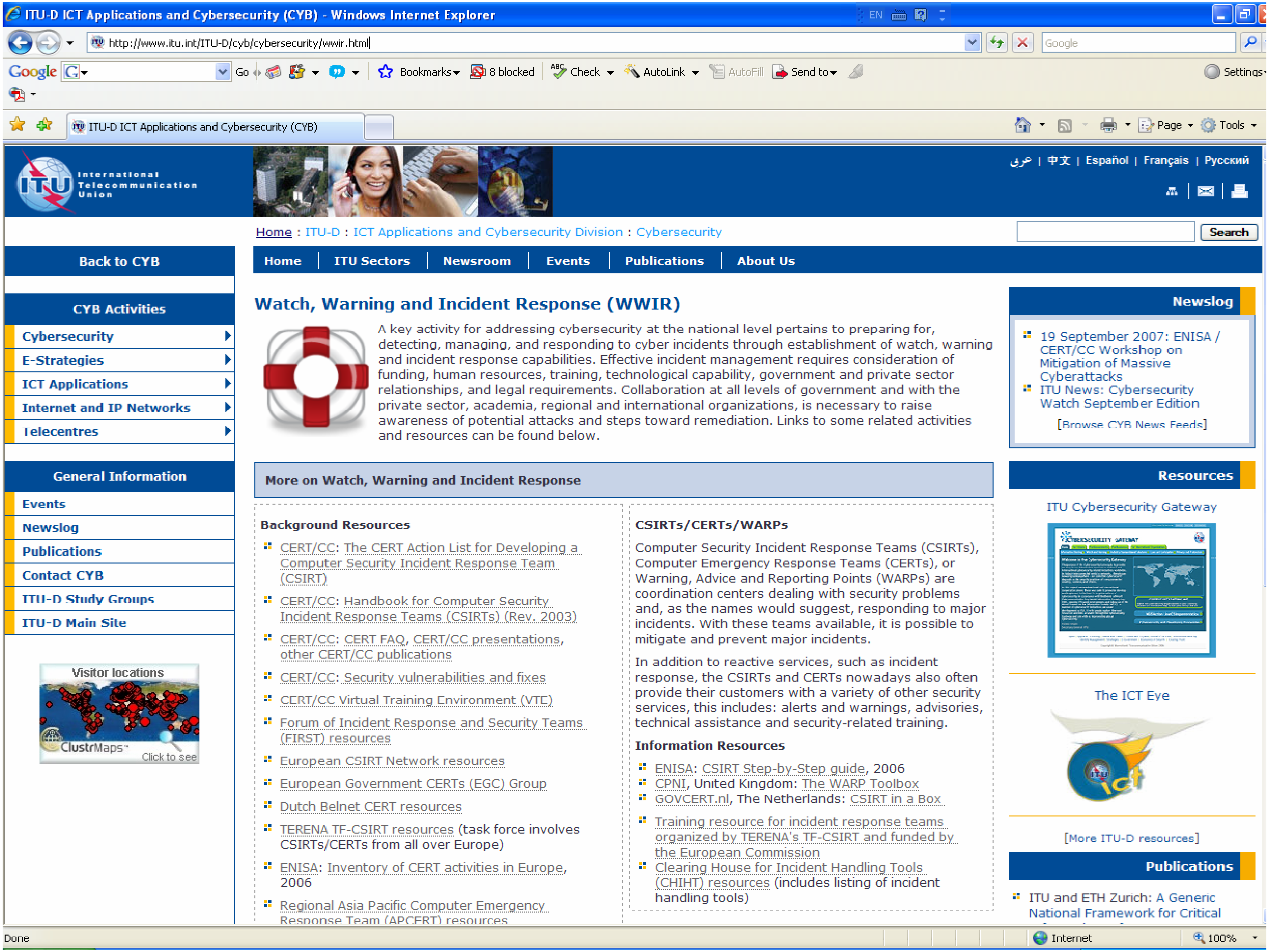
November 2007 DRAFT

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

Establishment of Watch, Warning and Incident Response (WWIR) Capabilities

- Assistance to Developing Countries related to Establishment of Watch, Warning and Incident Response (WWIR) Capabilities
- CSIRT Primer and Survey
- CSIRT Toolkit
- Inventory of Watch, Warning and Incident Response Capabilities by Region
- Standard Reporting Format for Fraudulent Online Activities (with e-crime extensions) (2008-2009)

- References
  - www.itu.int/ITU-D/cyb/cybersecurity/wwir.html


ITU-D ICT Applications and Cybersecurity (CYB) - Windows Internet Explorer
http://www.itu.int/ITU-D/cyb/cybersecurity/wwir.html
Google
Go
Bookmarks
8 blocked
Check
AutoLink
AutoFill
Send to
Settings
ITU-D ICT Applications and Cybersecurity (CYB)
Page
Tools
International Telecommunication Union
عربي | 中文 | Español | Français | Русский
Search
Home | ITU Sectors | Newsroom | Events | Publications | About Us
Back to CYB
Visitor locations
ClustrMaps
Click to see
Done
Internet
100%

Home : ITU-D : ICT Applications and Cybersecurity Division : Cybersecurity

CYB Activities

- Cybersecurity
- E-Strategies
- ICT Applications
- Internet and IP Networks
- Telecentres

General Information

- Events
- Newslog
- Publications
- Contact CYB
- ITU-D Study Groups
- ITU-D Main Site

Watch, Warning and Incident Response (WWIR)

A key activity for addressing cybersecurity at the national level pertains to preparing for, detecting, managing, and responding to cyber incidents through establishment of watch, warning and incident response capabilities. Effective incident management requires consideration of funding, human resources, training, technological capability, government and private sector relationships, and legal requirements. Collaboration at all levels of government and with the private sector, academia, regional and international organizations, is necessary to raise awareness of potential attacks and steps toward remediation. Links to some related activities and resources can be found below.

More on Watch, Warning and Incident Response

Background Resources

- CERT/CC: The CERT Action List for Developing a Computer Security Incident Response Team (CSIRT)
- CERT/CC: Handbook for Computer Security Incident Response Teams (CSIRTs) (Rev. 2003)
- CERT/CC: CERT FAQ, CERT/CC presentations, other CERT/CC publications
- CERT/CC: Security vulnerabilities and fixes
- CERT/CC Virtual Training Environment (VTE)
- Forum of Incident Response and Security Teams (FIRST) resources
- European CSIRT Network resources
- European Government CERTs (EGC) Group
- Dutch Belnet CERT resources
- TERENA TF-CSIRT resources (task force involves CSIRTs/CERTs from all over Europe)
- ENISA: Inventory of CERT activities in Europe, 2006
- Regional Asia Pacific Computer Emergency Response Team (APCERT) resources

CSIRTs/CERTs/WARPs

Computer Security Incident Response Teams (CSIRTs), Computer Emergency Response Teams (CERTs), or Warning, Advice and Reporting Points (WARPs) are coordination centers dealing with security problems and, as the names would suggest, responding to major incidents. With these teams available, it is possible to mitigate and prevent major incidents.

In addition to reactive services, such as incident response, the CSIRTs and CERTs nowadays also often provide their customers with a variety of other security services, this includes: alerts and warnings, advisories, technical assistance and security-related training.

Information Resources

- ENISA: CSIRT Step-by-Step guide, 2006
- CPNI, United Kingdom: The WARP Toolbox
- GOVCERT.nl, The Netherlands: CSIRT in a Box
- Training resource for incident response teams organized by TERENA's TF-CSIRT and funded by the European Commission
- Clearing House for Incident Handling Tools (CHIHT) resources (includes listing of incident handling tools)

Newslog

- 19 September 2007: ENISA / CERT/CC Workshop on Mitigation of Massive Cyberattacks
- ITU News: Cybersecurity Watch September Edition

[Browse CYB News Feeds]

Resources

ITU Cybersecurity Gateway

The ICT Eye

[More ITU-D resources]

Publications

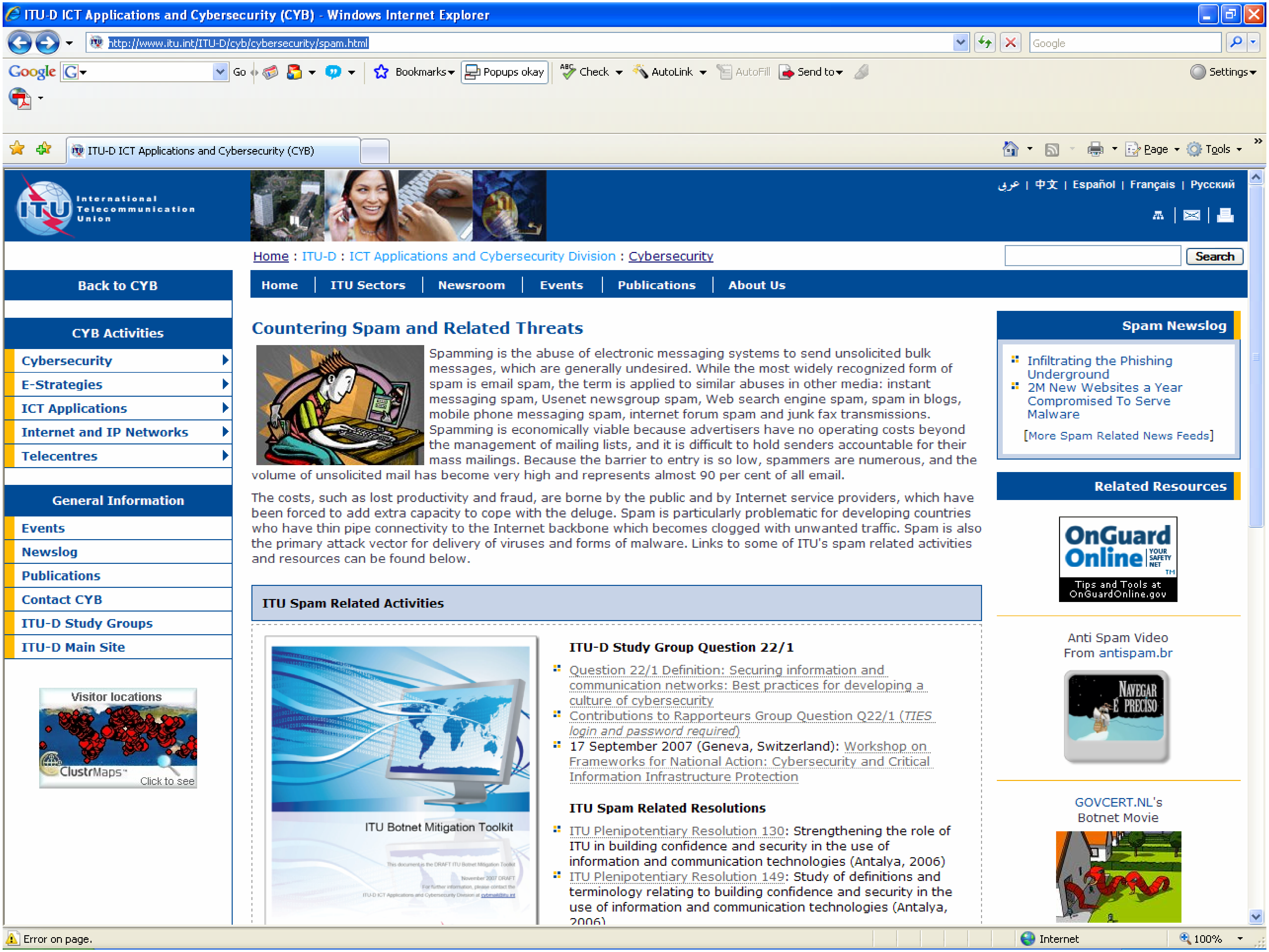
- ITU and ETH Zurich: A Generic National Framework for Critical

Information Sharing through Enhancing the ITU Cybersecurity Gateway

- Enhancement of the ITU Cybersecurity Gateway
- Establishment of an ITU Cybersecurity/CIIP Directory
- Establishment of an ITU Cybersecurity/CIIP Contact Database
- Establishment of Annual Who's Who in Cybersecurity/CIIP Publication
- Establishment of an Annual ITU Cybersecurity Publication
- ITU Cybersecurity Fellowship Programme for Developing Countries
- References
  - http://www.itu.int/cybersecurity/gateway/

Countering Spam and Related Threats

- Survey on Anti-Spam Legislation Worldwide (underway)
- Botnet Mitigation Toolkit for Developing Countries
  - Pilot Projects for Implementation of Toolkit (Malaysia)
- Joint Activities for StopSpamAlliance.org
- Study on Financial Aspects of Spam and Malware (with ITU-T Study Group 3)
- Translation of Message Anti-Abuse Working Group Best Practices Docs (almost completed)
  - Code of Conduct
  - MAAWG - Managing Port25
  - BIAC-MAAWG Best Practices Expansion Document
  - Anti-Phishing Best Practices for ISPs and Mailbox Providers
  - MAAWG Sender BCP Version 1.1 & Executive Summary
- References
  - http://www.itu.int/ITU-D/cyb/cybersecurity/spam.html


ITU-D ICT Applications and Cybersecurity (CYB) - Windows Internet Explorer
http://www.itu.int/ITU-D/cyb/cybersecurity/spam.html
Google
Go
Bookmarks
Popups okay
Check
AutoLink
AutoFill
Send to
Settings
ITU-D ICT Applications and Cybersecurity (CYB)
Page
Tools
Error on page.
Internet
100%

Back to CYB

CYB Activities

- Cybersecurity
- E-Strategies
- ICT Applications
- Internet and IP Networks
- Telecentres

General Information

- Events
- Newslog
- Publications
- Contact CYB
- ITU-D Study Groups
- ITU-D Main Site

Visitor locations

ClustrMaps

Click to see

Countering Spam and Related Threats

Spamming is the abuse of electronic messaging systems to send unsolicited bulk messages, which are generally undesired. While the most widely recognized form of spam is email spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, mobile phone messaging spam, internet forum spam and junk fax transmissions. Spamming is economically viable because advertisers have no operating costs beyond the management of mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high and represents almost 90 per cent of all email.

The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers, which have been forced to add extra capacity to cope with the deluge. Spam is particularly problematic for developing countries who have thin pipe connectivity to the Internet backbone which becomes clogged with unwanted traffic. Spam is also the primary attack vector for delivery of viruses and forms of malware. Links to some of ITU's spam related activities and resources can be found below.

ITU Spam Related Activities

ITU Botnet Mitigation Toolkit

ITU-D Study Group Question 22/1

- Question 22/1 Definition: Securing information and communication networks: Best practices for developing a culture of cybersecurity
- Contributions to Rapporteurs Group Question Q22/1 (*TIES login and password required*)
- 17 September 2007 (Geneva, Switzerland): Workshop on Frameworks for National Action: Cybersecurity and Critical Information Infrastructure Protection

ITU Spam Related Resolutions

- ITU Plenipotentiary Resolution 130: Strengthening the role of ITU in building confidence and security in the use of information and communication technologies (Antalya, 2006)
- ITU Plenipotentiary Resolution 149: Study of definitions and terminology relating to building confidence and security in the use of information and communication technologies (Antalya, 2006)

Spam Newslog

- Infiltrating the Phishing Underground
- 2M New Websites a Year Compromised To Serve Malware

[More Spam Related News Feeds]

Related Resources

OnGuard Online YOUR SAFETY NET TM Tips and Tools at OnGuardOnline.gov

Anti Spam Video From antispam.br

NAVEGAR É PRECISO

GOVCERT.NL's Botnet Movie

Case Study: Spam, Malware, Botnets

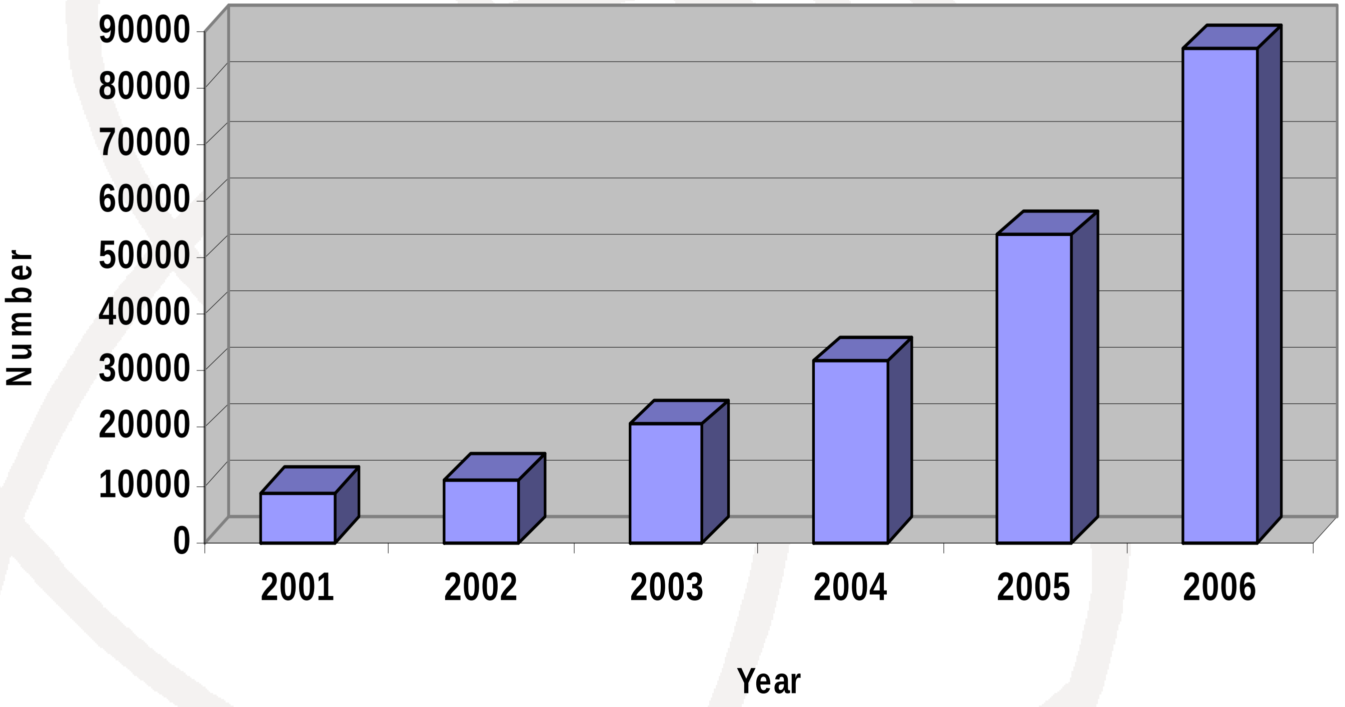
ITU Study on Financial Aspects of Network Security: Malware & Spam

- Malware and spam are converging: spam is used to expand and sustain botnets, which are, in turn, used to send spam
- Negative and positive financial effects
  - Costs for individuals, organizations, nations
  - Benefits for legal but also illegal players
- Study aims at documenting the state of knowledge of these financial aspects

Economics of Security

- New international “division of labor” contributes to cheap yet increasingly sophisticated forms of attacks
- Net profits of fraudulent and criminal activity are presently high, contributing to expanding security violations
- Better empirical information basis is required for more effective counter-measures

New malware releases



Source: Kasperski Labs, 2007

An economic perspective

- Highly complex interactions in the information and communication technology (ICT) value net
- Legitimate and illegitimate players act rational, responding to (perceived) economic incentives
- Security failures caused by misaligned economic incentives as much as bad technical design or careless user behavior

“Benefits”

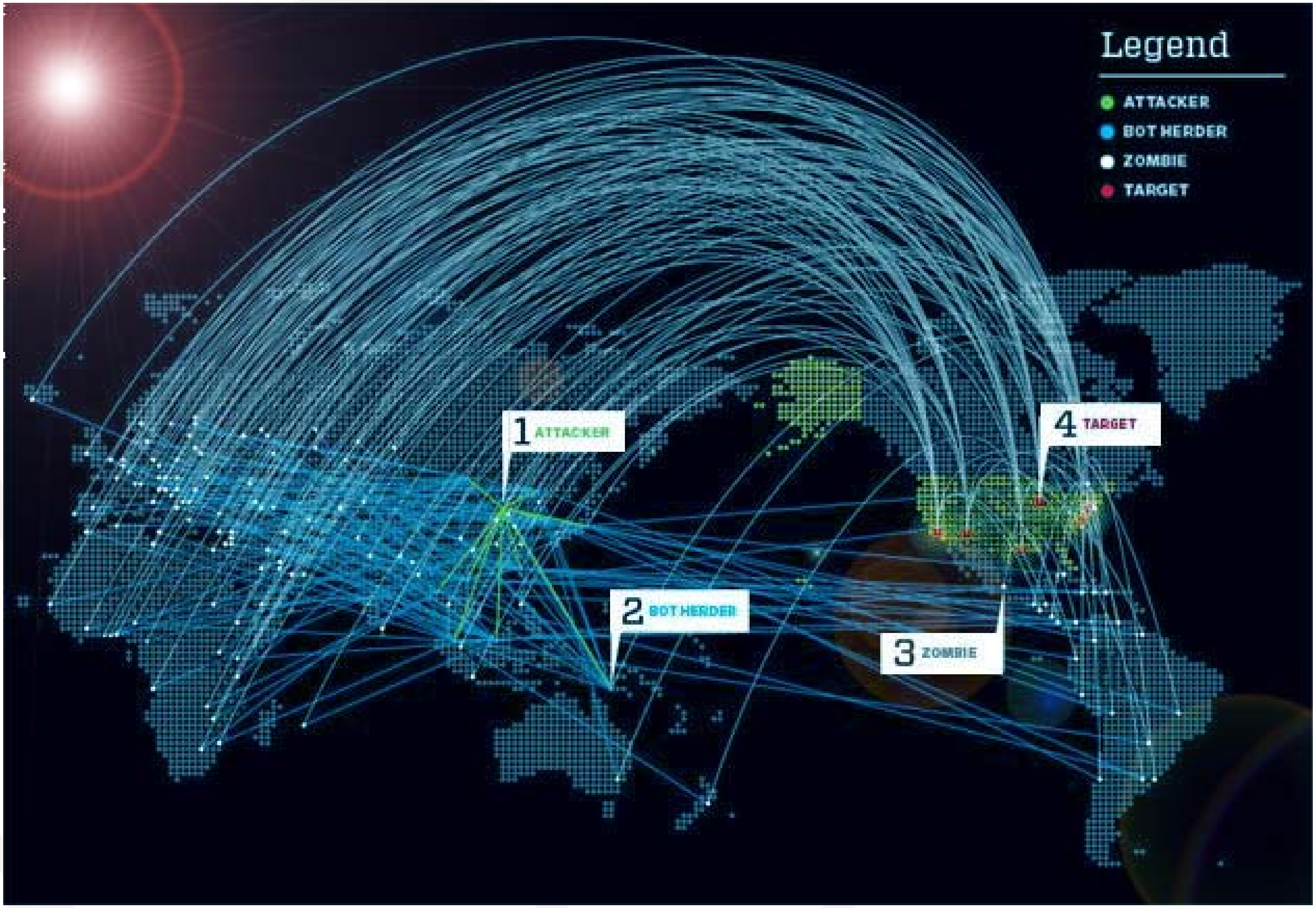
- Legal business opportunities
  - Security software and services
  - Infrastructure equipment and bandwidth
- Illegal business opportunities
  - Writing of malicious code
  - Renting of botnets
  - Profits from pump and dump stock schemes
  - Commission on spam-induced sales
  - Sales of illegally acquired goods
  - Money laundering

Outline of Study (March 2008)

- Principal investigators:
  - Dr. Michel J. G. van Eeten, Delft University of Technology, The Netherlands
  - Dr. Johannes M. Bauer, Michigan State University, USA
- The problem of malware
- Business models related to malware
- Financial aspects of malware
- Financial aspects of spam
- Preliminary assessment of welfare effects

Case Study: Botnets

- Botnets (also called zombie armies or drone armies) are networks of compromised computers infected with viruses or malware to turn them into “zombies” or “robots” — without the owners’ knowledge.
- 2007 generation botnets such as Zhelatin (Storm Worm) are particularly aggressive using advanced techniques such as fast-flux networks and striking back with denial of service (DDOS) attacks against security researchers or vendors trying to mitigate botnet
  - *"Fast-flux service networks are a network of compromised computer systems with public DNS records that are constantly changing, in some cases every few minutes. These constantly changing architectures make it much more difficult to track down criminal activities and shut down their operations.“*
    - Honeynet Project & Research Alliance



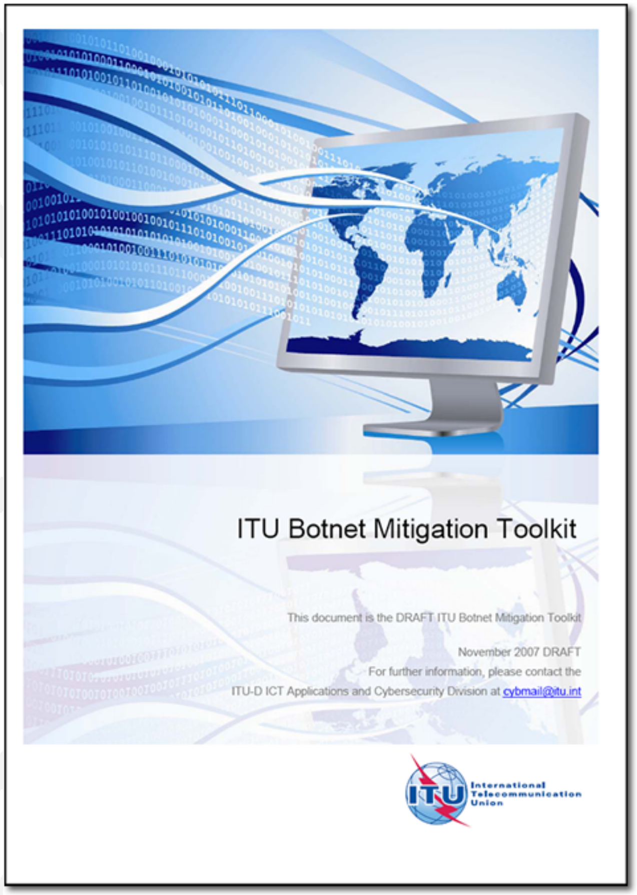
Source: Wired Magazine

ITU Botnet Mitigation Project inspired by Australian Internet Security Initiative (AISI)

- Australian Communications and Media Authority (ACMA) partnership with 25 Australian ISPs
  - ACMA collects data on IPs emitting malware
    - Identifies IPs operated by participating Australian ISPs
    - Notifies ISP responsible for affected IPs
  - ISPs undertake to mitigate malware activity from infected IPs on their networks
    - Notify infected customers
    - Change security and filtering policies as necessary
- AISI project working internationally to fight botnets and has agreed to assist ITU project and extend AISI to other ITU Member States

ITU Botnet Mitigation Package

- Framework for national botnet related policy, regulation and enforcement
- Multi-stakeholder international cooperation and outreach
  - Phase 1 (2007): Downloadable toolkit/guidelines for ITU Member States
  - Phase 2 (2008/2009): Targeted national/regional assistance initiatives
    - Malaysia, TBD



ITU Botnet Mitigation Toolkit

This document is the DRAFT ITU Botnet Mitigation Toolkit

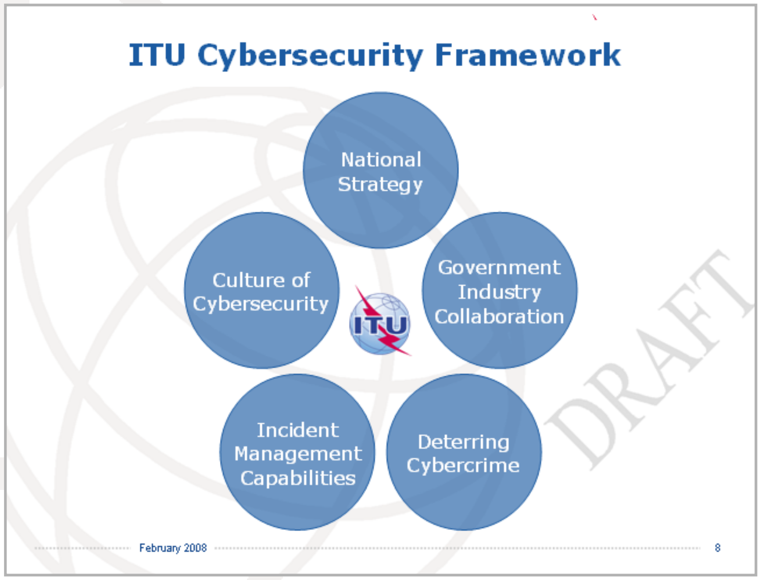
November 2007 DRAFT

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

Recap of Desired Outcomes of this Event

Explain the ITU Cybersecurity Framework

- To identify major cybersecurity actors in a country, their roles and means of coordination, interaction, and cooperation…



ITU Cybersecurity Framework

National Strategy
Government Industry Collaboration
Deterring Cybercrime
Incident Management Capabilities
Culture of Cybersecurity
ITU

February 2008 8

Including those who…

- Lead government interagency efforts on cybersecurity and provide operational guidance;
- Interact with the private sector with regards to cybersecurity whether for cybercrime, incident management, or technical and policy development;
- Develop and enforce laws related to cybersecurity;
- Coordinate action related to the prevention of, preparation for, response to, and recovery from cyber incidents; and,
- Promote a national culture of cybersecurity, including awareness-raising for individuals, small businesses and other users.

More Information

- ITU-D ICT Applications and Cybersecurity Division
  - www.itu.int/itu-d/cyb/
- ITU-D Cybersecurity Overview
  - www.itu.int/itu-d/cyb/cybersecurity/
- Study Group Q.22/1: Report On Best Practices For A National Approach To Cybersecurity: A Management Framework For Organizing National Cybersecurity Efforts
  - www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf
- National Cybersecurity/CIIP Self-Assessment Toolkit
  - www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
- ITU-D Cybersecurity Work Programme to Assist Developing Countries:
  - www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf
- Regional Cybersecurity Forums
  - www.itu.int/ITU-D/cyb/events/
- Botnet Mitigation Toolkit
  - http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

International Telecommunication Union

Helping the World Communicate