ITU and Cybersescurity

Pablo Palacios
Programme Officer
ITU Area Office located in Chile
International Telecommunications Union

4 December 2018

About ITU

ITU is the United Nations **specialized agency for information and communication technologies** (ICTs)

Founded in Paris in 1865 as the International Telegraph Union

More than 153 years of experience and innovation

ITU members

193

MEMBER STATES

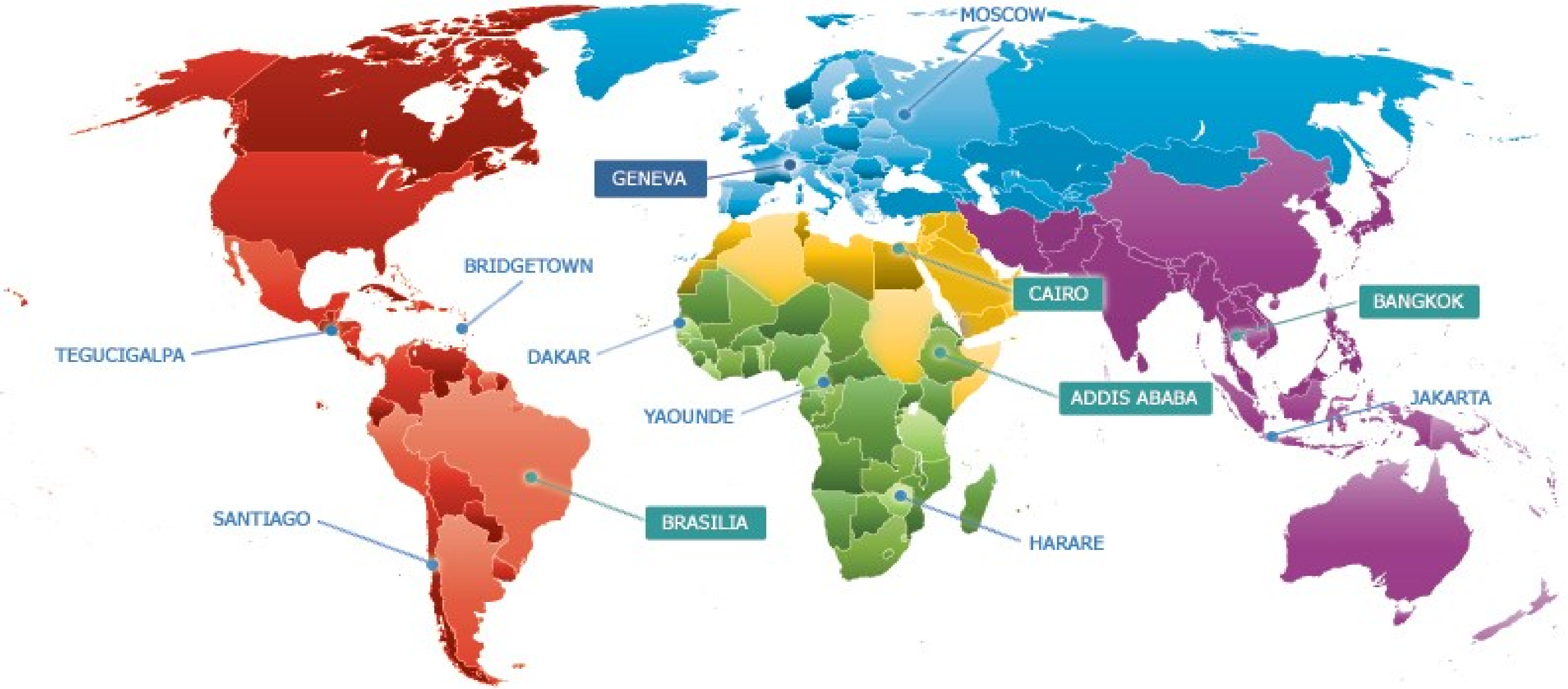
+700

INDUSTRY & INTERNATIONAL ORGANIZATIONS

+150

ACADEMIA MEMBERS

ITU’s Regional Offices



ITU's Structure

Radiocommunication
ITU-R

Coordinates global wireless communication

Standardization
ITU-T

Produces interoperable technical ICT standards

Development
ITU-D

Provides assistance to the un-connected

The General Secretariat provides intersectorial coordination for the whole organization

WHAT IS NEW?

Artificial Intelligence!!!

Industry leaders call 5G and Artificial Intelligence emblematic of the shift to a smarter society

5G update: New ITU standards for network softwarization and fixed-mobile convergence

The “Artificial Intelligence of Everything” is the top tech trend for 2017 and could be an inflection point for humankind and the SDGs

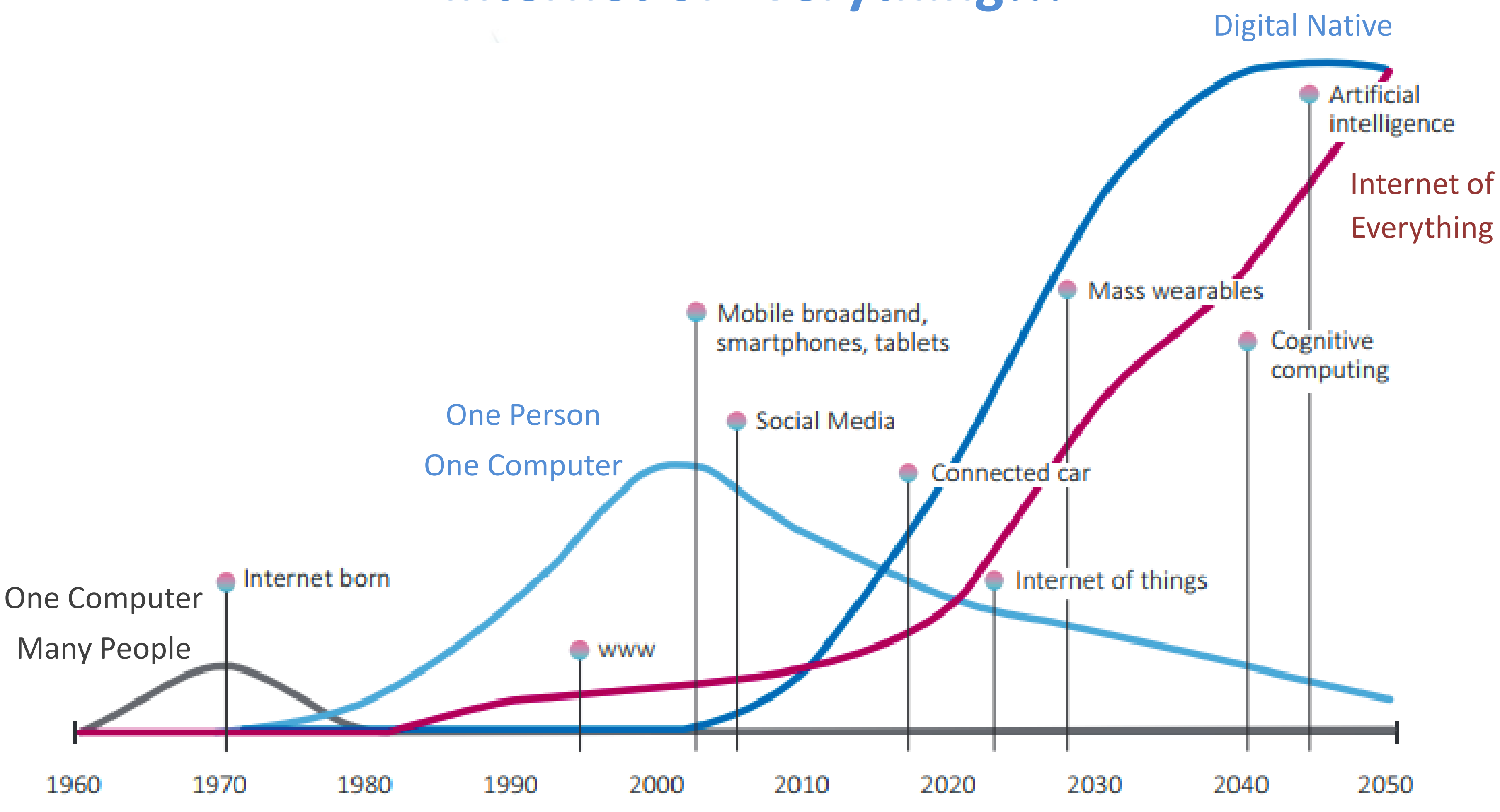
ITU launches new Focus Group to study Machine Learning for Future Networks including 5G

Security and privacy by design, open APIs, network virtualization, identity and authorization, analytics and accessibility have been identified by industry leaders as core principles to guide ITU standardization work towards 2020

Work Item Y.SSC-AISE-arc: Reference architecture of artificial intelligence service exposure for smart sustainable cities

Work Item TR.AI4IoT (ex Y.AI4SC): Artificial Intelligence and Internet of Things

Internet of Everything!!!



ITU: Trends in Telecommunication Reform 2015, Getting Ready for the Digital Economy

Everything is getting interconnected!!!

Increasing Broadband access
Ubiquitous World

New applications in all areas

e-health / e-learning

e-government / e-commerce

e-banking / e-money

Entertainment / Media

Social networks

Communications in Disasters / GPS

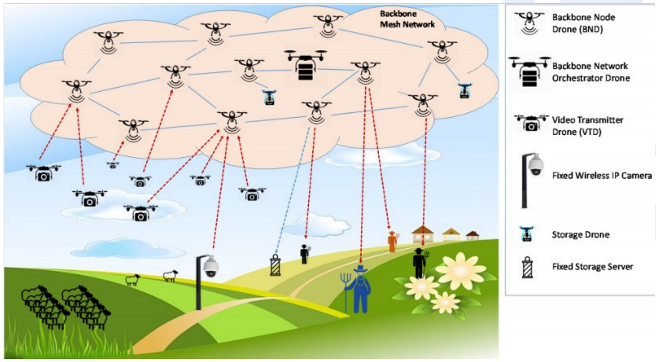
Agriculture

Accessibility

Increasing connections M2M

IoT – Internet of Everything

smarter sensors



Backbone Mesh Network
Backbone Node Drone (BND)
Backbone Network Orchestrator Drone
Video Transmitter Drone (VTD)
Fixed Wireless IP Camera
Storage Drone
Fixed Storage Server

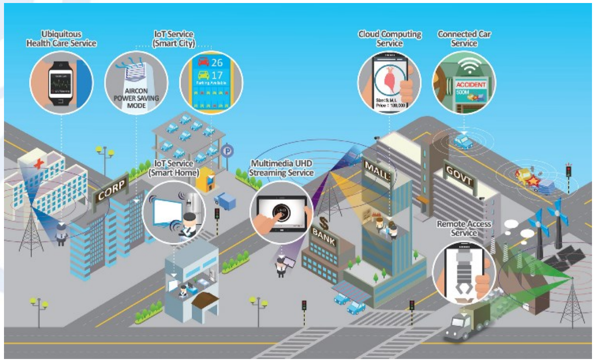
Drones is its applications

Artificial Intelligence / Robots

Autonomous Cars

Smart Homes / Smart Cities

Etc.



5G networks / Smart Cities
Cloud Computing / Big Data

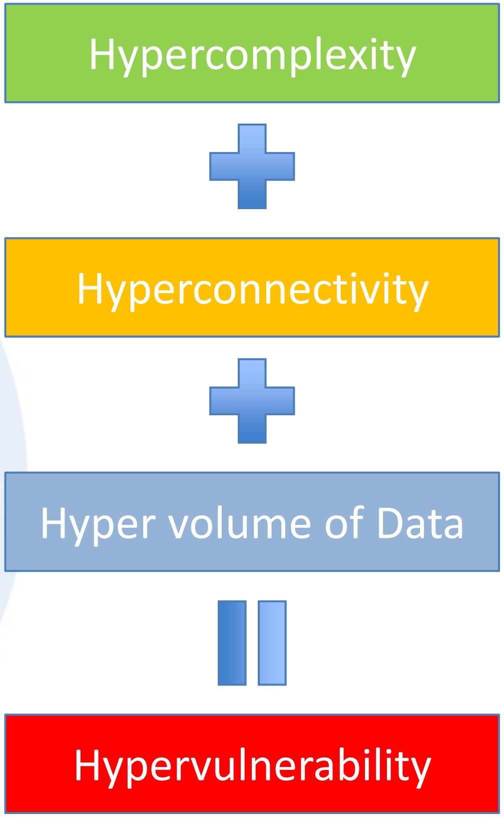
Smart Cities

Connecting more and more components of the city for efficiency and sustainability of urban processes

Smart stop Lights, smart sensors, smart traffic, smart water, smart electricity grids, etc.

Each new Connection opens a new door for Cyberattacks

ITU Magazine No2 2016 Building Smart and Sustainable Cities for tomorrow



Hypercomplexity

+

Hyperconnectivity

+

Hyper volume of Data

=

Hypervulnerability

Traditional TICs
IoT / M2M / Bluetooth
Cloud Computing / Big Data

Example: Smart Autonomous Car

ITU Magazine No2 2016 Building Smart and Sustainable Cities for tomorrow

Example: How Smart is the Smart Water Management?

Efficiency

Quality and contamination Control

Finance Management

Smart distribution of the water

Information Management

Monitor and prevent emergencies

ITU Magazine No2 2016 Building Smart and Sustainable Cities for tomorrow

e-banking and e-money

e-banking

Online banking services offered through mobile cell phones. It is needed a Banking account

Digital Financial Services

Use of ICTs to wide the offer of financial services. It is not needed a bank account.

It is used agents for payments and to manage the cash transactions. It is used mobiles and other digital means for the transactions.

Critical Factors for Success

Interoperability

Impact of the Technology

Regulations

Risks for the Consumer

Cybersecurity issues

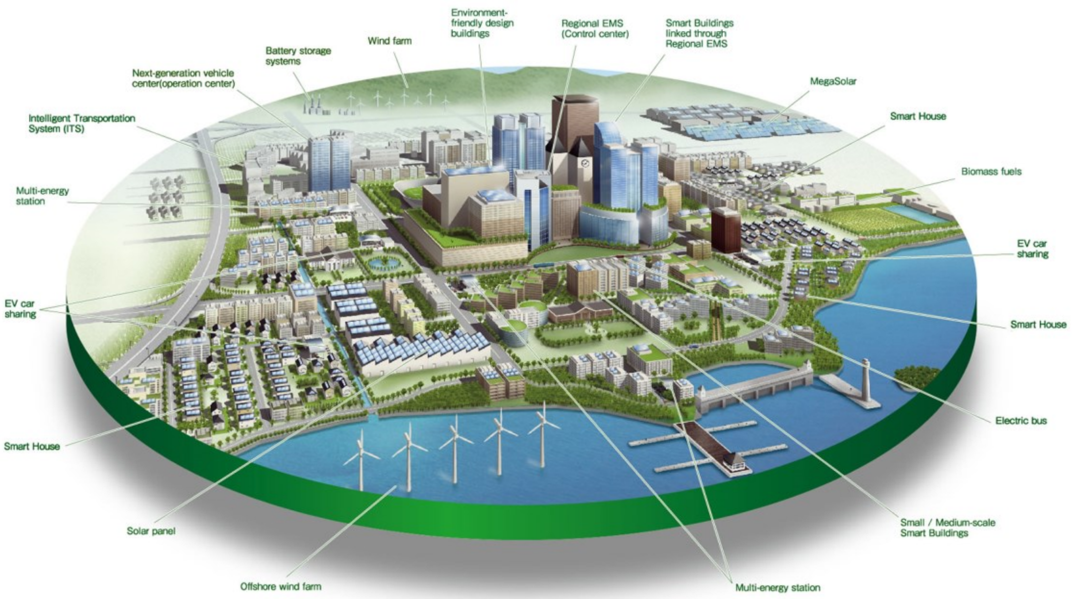
Easy Use

e-money *

“Electronic money is an electronic store of monetary value on a technical device that may be widely used for making payments to entities other than the e-money issuer. The device acts as a prepaid bearer instrument which does not necessarily involve bank accounts in transactions. E-money products can be hardware-based or software-based, depending on the technology used to store the monetary value.”

* European Central Bank: https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html

What is considered as Critical Infrastructure?


Environment-friendly design buildings
Regional EMS (Control center)
Smart Buildings linked through Regional EMS
Wind farm
Battery storage systems
Next-generation vehicle center(operation center)
MegaSolar
Intelligent Transportation System (ITS)
Smart House
Biomass fuels
Multi-energy station
EV car sharing
EV car sharing
Smart House
Electric bus
Smart House
Solar panel
Small / Medium-scale Smart Buildings
Offshore wind farm
Multi-energy station

Electrical System

Gas System

Oil System

Industrial Sector

Water System

Agriculture

Health

National Telecommunications Systems

Transportation

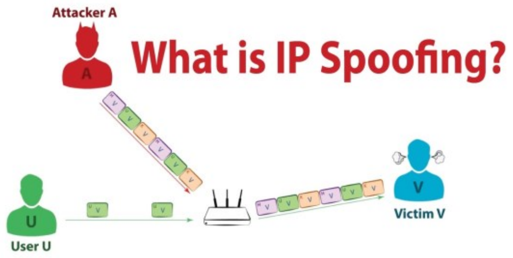
Financial System

Police, Army, City Security

Chemistry Sector

What are the Cyberthreats!!!

CyberAttacks and Hacking



IP Spoofing

Fishing

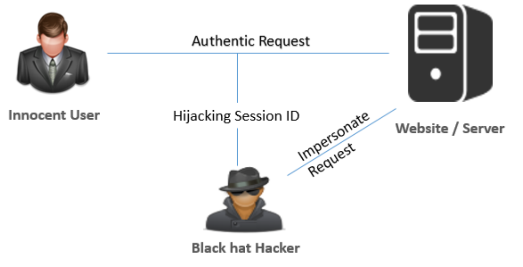
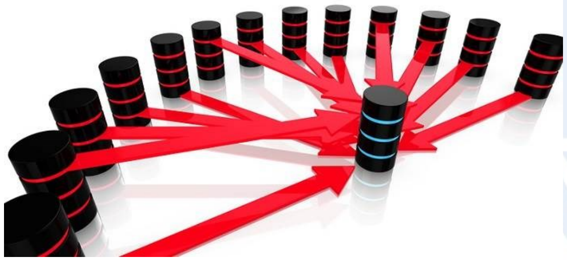
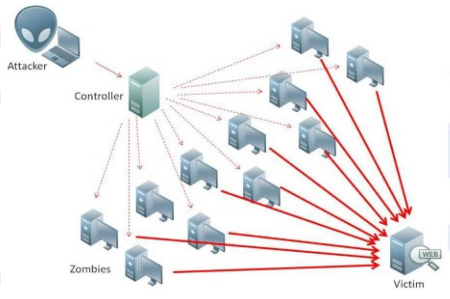


Image created by Sarvesh Kushwaha

Session Hijacking
Man-in-the-Middle



DoS



DDoS, rDoS

Social Engineering

Ramsomeware Exploits SQL injection Credential Reuse

Virus Worms Spyware Spam

Threat Intelligence

“Details of the motivations, intent, and capabilities of internal and external threat actors. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats.” *

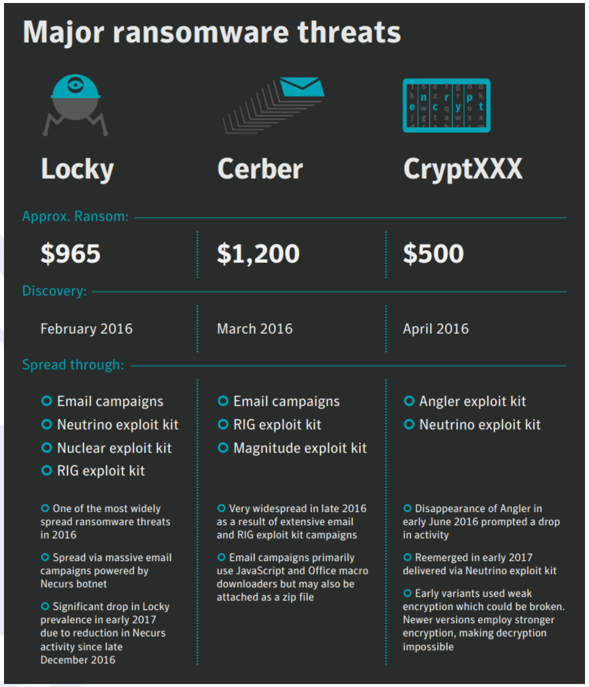
- **Timely:** Needs time to perform the actions;
- **Accurate:** the number of false positive alerts or actions obtained from the threat intelligence;
- **Relevant:** how the intelligence is organized and delivered to ensure it addresses the industry;
- **Tailored:** must be provided to different people to enable them to make the decisions relevant to their role.**

* Forrester / ** Silensec

Ransomware

Malware which action limits users to access to their system and information. The Ransomware can lock the system's screen or can lock the users' files; as a result, it is requested a ransom to be paid.

New versions of ransomware, as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key. *



Major ransomware threats

	Locky	Cerber	CryptXXX
Approx. Ransom:	$965	$1,200	$500
Discovery:	February 2016	March 2016	April 2016
Spread through:	○ Email campaigns ○ Neutrino exploit kit ○ Nuclear exploit kit ○ RIG exploit kit	○ Email campaigns ○ RIG exploit kit ○ Magnitude exploit kit	○ Angler exploit kit ○ Neutrino exploit kit
	○ One of the most widely spread ransomware threats in 2016 ○ Spread via massive email campaigns powered by Necurs botnet ○ Significant drop in Locky prevalence in early 2017 due to reduction in Necurs activity since late December 2016	○ Very widespread in late 2016 as a result of extensive email and RIG exploit kit campaigns ○ Email campaigns primarily use JavaScript and Office macro downloaders but may also be attached as a zip file	○ Disappearance of Angler in early June 2016 prompted a drop in activity ○ Reemerged in early 2017 delivered via Neutrino exploit kit ○ Early variants used weak encryption which could be broken. Newer versions employ stronger encryption, making decryption impossible

"Due to its prevalence and destructiveness, ransomware remained the most dangerous cyber crime threat facing consumers and businesses in 2016. The average ransom amount has shot upwards, jumping 266 percent from US$294 in 2015 to $1,077. Attackers clearly think that there's more to be squeezed from victims. Detections of ransomware increased by 36 percent in 2016." **

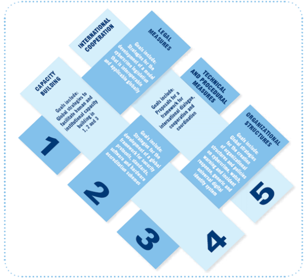
*TrendMicro: https://www.trendmicro.com/vinfo/us/security/definition/ransomware / ** Symantec: Internet Security Threat Report, April 2017, Volume 22

Cybersecurity!!!

ITU Mandate on Cybersecurity

2003 – 2005
WSIS entrusted ITU as sole facilitator for WSIS Action Line C5 - “**Building Confidence and Security in the use of ICTs**”

world summit
on the **information society**
Geneva 2003 - Tunis 2005



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: Strategies for the development of a global framework for security protocols, standards, software and hardware accreditation schemes
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
1
2
3
4
5

2007
Global Cybersecurity Agenda (GCA) was launched by ITU Secretary General
GCA is a **framework for international cooperation in cybersecurity**

2008 to date
ITU Membership endorsed the GCA as the ITU-wide strategy on international cooperation.

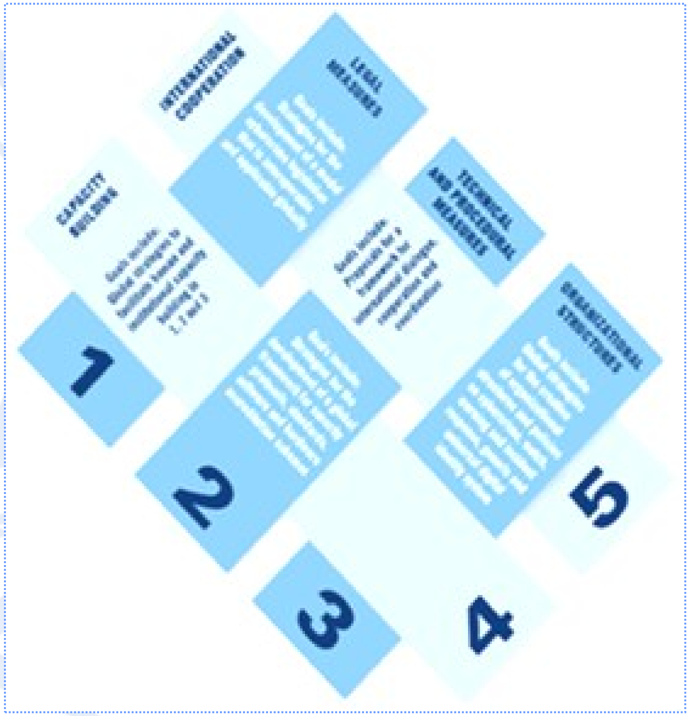
GCA GLOBAL CYBERSECURITY AGENDA

Child Online Protection

Building confidence and security in the use of ICTs is widely present in **PP and Conferences**’ resolutions. In particular WTSA 12, PP 10 and WTDC 10 produced Resolutions (WTSA 12 Res 50, 52, 58, PP Res 130, 174, 179, 181 and WTDC 45 and 69) which touch on the most relevant ICT security related issues, from legal to policy, to technical and organization measures.

Global Cybersecurity Agenda (GCA)

- GCA is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners, and building on existing initiatives to avoid duplicating efforts.
- GCA builds upon five pillars:
  1. Legal Measures
  2. Technical and Procedural Measures
  3. Organizational Structure
  4. Capacity Building
  5. International Cooperation
- Since its launch, GCA has attracted the support and recognition of leaders and cybersecurity experts around the world.


INTERNATIONAL COOPERATION
LEGAL MEASURES
CAPACITY BUILDING
TECHNICAL AND PROCEDURAL MEASURES
ORGANIZATIONAL STRUCTURES
1
2
3
4
5

24 Indicators based on the 5 pillars of the Global Cybersecurity Agenda (GCA)

Legal

- Cybercriminal legislation
- Cybersecurity regulation
- Cybersecurity training on regulation and laws

Technical

- National CIRT
- Government CIRT
- Sectoral CIRT
- Standards implementation framework for organizations
- Standards and certification for professionals

Organizational

- Strategy
- Responsible agency
- Cybersecurity metrics

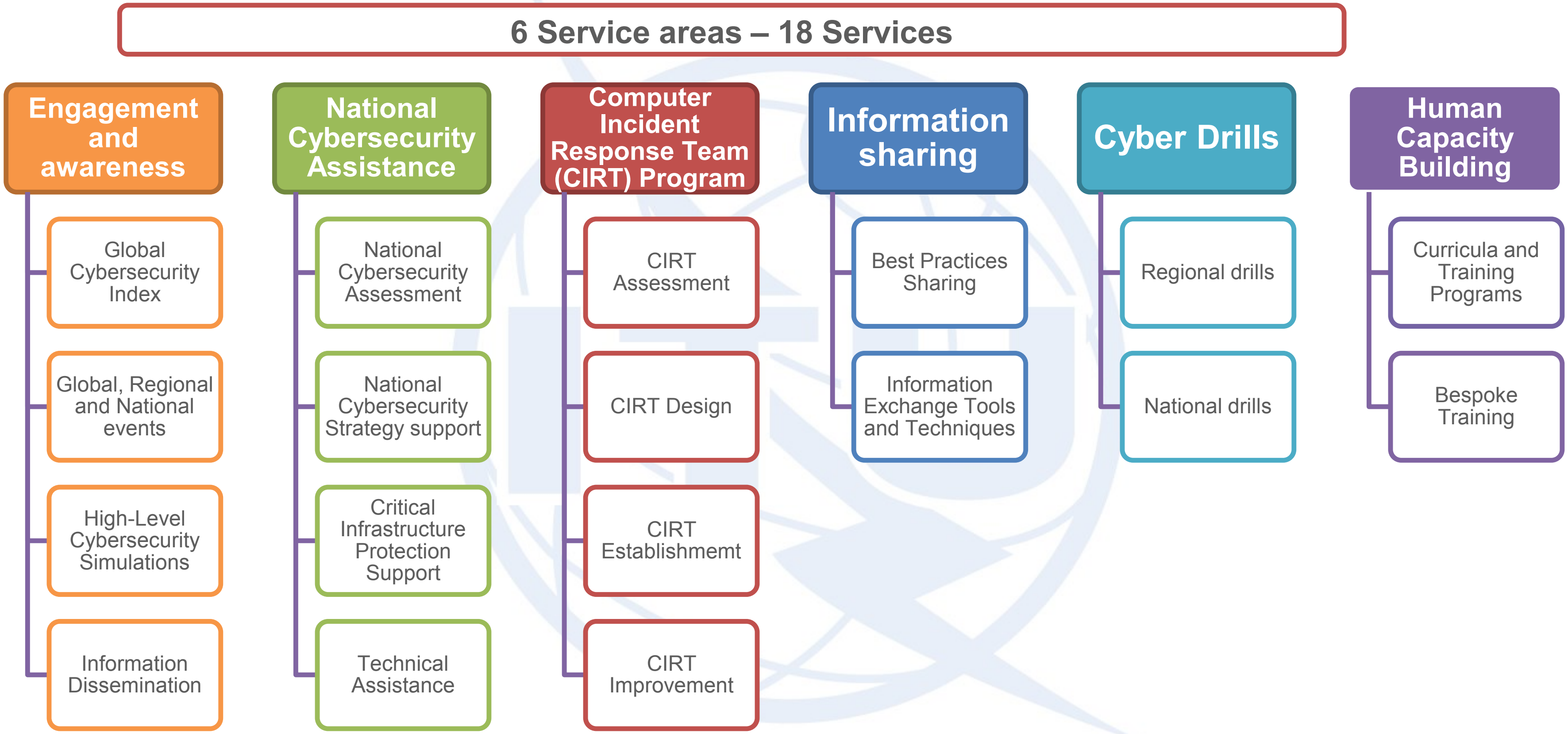
Capacity Building

- Standardization bodies
- Best practice
- R & D programmes
- Public awareness campaigns
- Professional training courses
- National education programmes and academic curricula
- Incentive mechanisms
- Home-grown cybersecurity industry

Cooperation

- Bilateral agreements
- Multilateral agreements
- International fora participation
- Public-private partnerships
- Interagency partnerships

BDT Cybersecurity Program



6 Service areas – 18 Services

Engagement and awareness

- Global Cybersecurity Index
- Global, Regional and National events
- High-Level Cybersecurity Simulations
- Information Dissemination

National Cybersecurity Assistance

- National Cybersecurity Assessment
- National Cybersecurity Strategy support
- Critical Infrastructure Protection Support
- Technical Assistance

Computer Incident Response Team (CIRT) Program

- CIRT Assessment
- CIRT Design
- CIRT Establishmemt
- CIRT Improvement

Information sharing

- Best Practices Sharing
- Information Exchange Tools and Techniques

Cyber Drills

- Regional drills
- National drills

Human Capacity Building

- Curricula and Training Programs
- Bespoke Training

What is Cybersecurity?

Tools

Guidelines

Assurance

Policies

Technologies

Actions Training

Best practices

Security concepts

Risk management

Security safeguards

Protect the Cyber Environment

Organization / User’s assets / Computing devices / Personnel / Infrastructure / Applications / Services / Telecommunications Systems

The totality of transmitted and/or stored information in the cyber environment

Objectives of Cybersecurity

Confidentiality

Availability

Integrity: Authenticity and Non-repudiation

Regulatory Issues: Market for Customers

Privacy

Fighting illegal and harmful content

Security

Delivery

Copyright

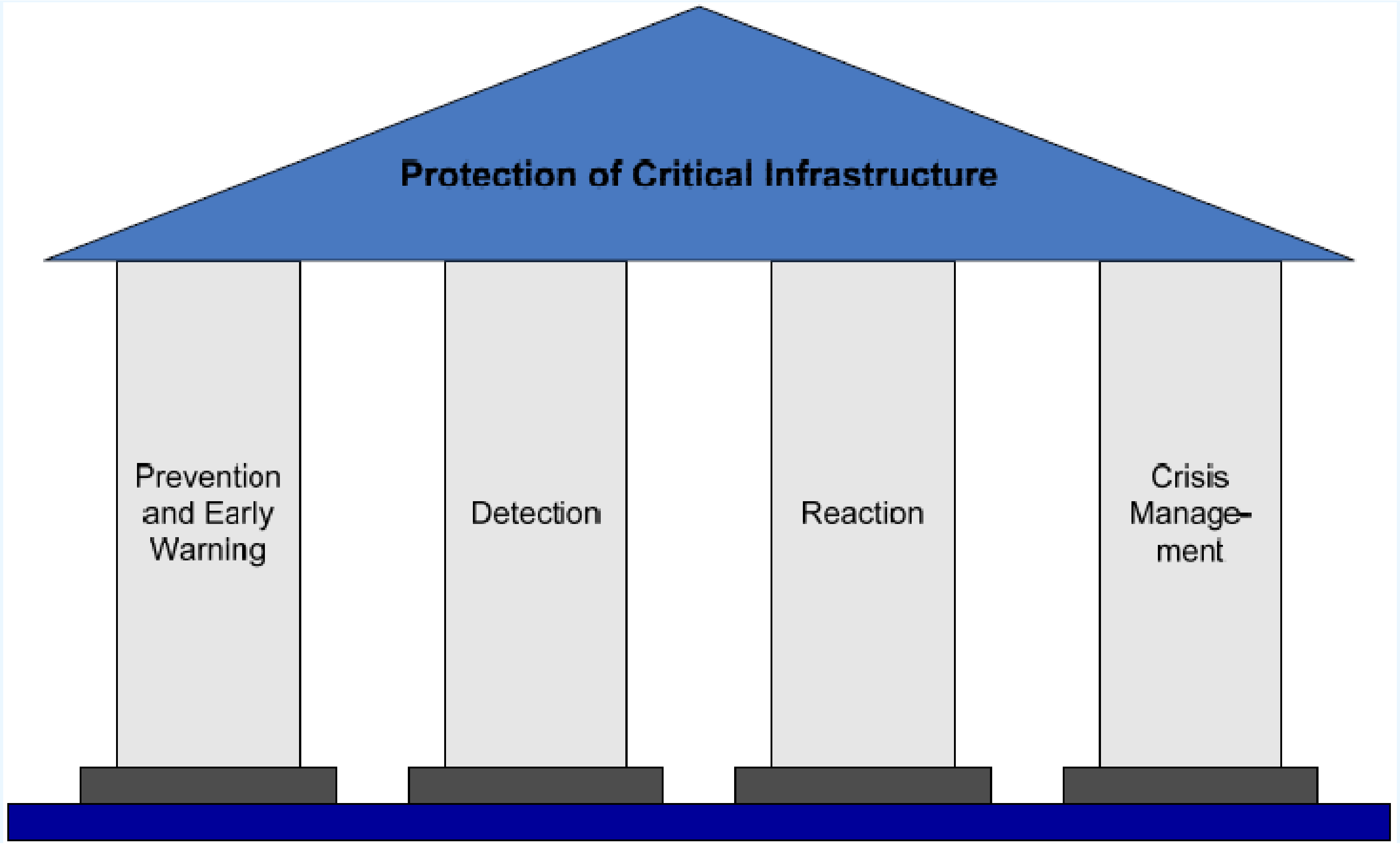
Net neutrality

Payments

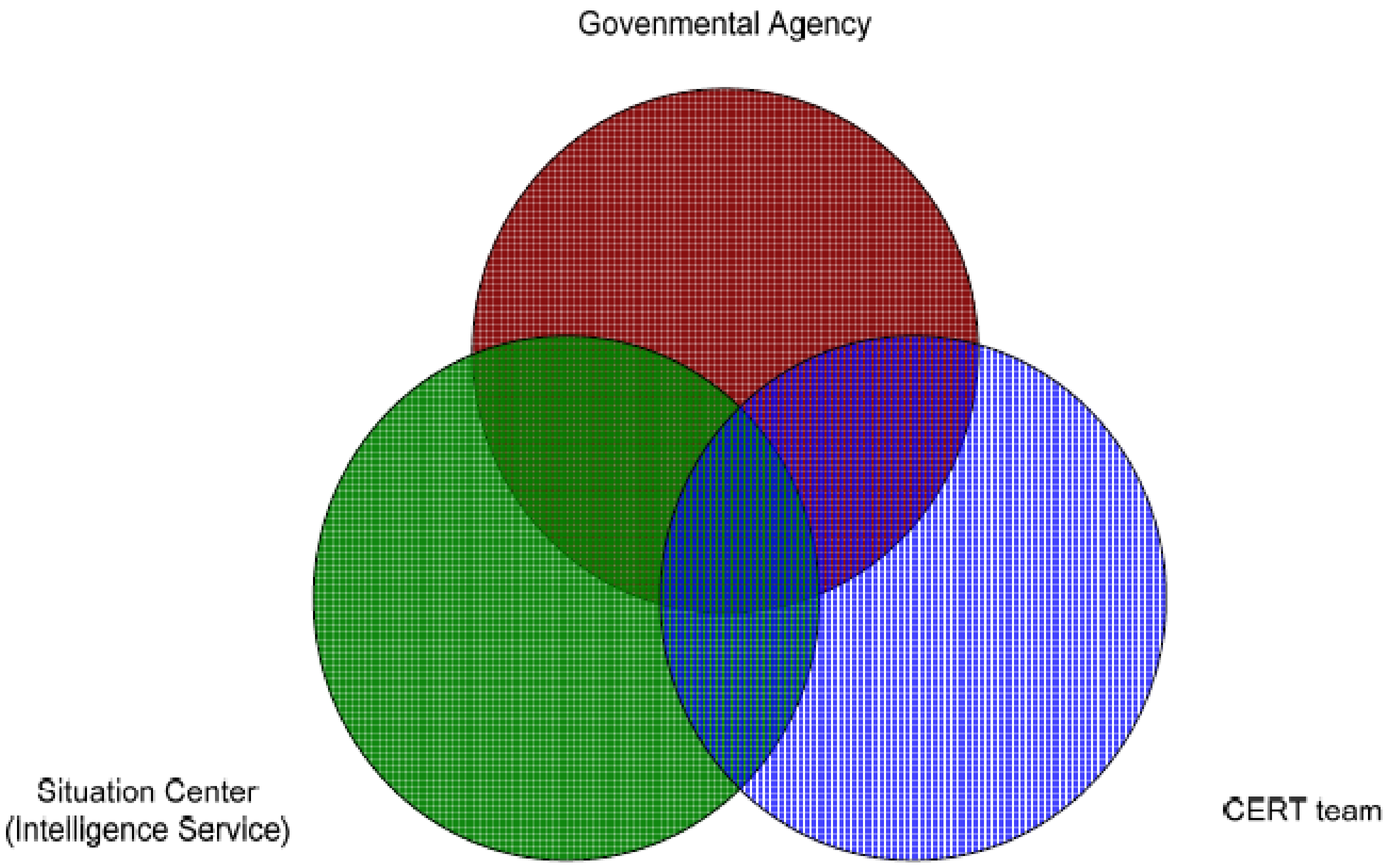
Consumer education

Consumer rights and trust

ITU: Trends in Telecommunication Reform 2015, Getting Ready for the Digital Economy


Protection of Critical Infrastructure
Prevention and Early Warning
Detection
Reaction
Crisis Manage-ment

Critical information infrastructure protection



A Generic National Framework For Critical Information Infrastructure Protection (CIIP)

BDT Cybersecurity Service Catalogue

Engagement and awareness

- Global Cybersecurity Index
- Global, Regional and National events
- Information dissemination

Computer Incident Response Team (CIRT) Program

- CIRT design
- CIRT implementation
- CIRT enhancement

Cyber Drills

- Regional drills
- National drills

Information sharing

- Best Practices Sharing
- Information Exchange Tools and Techniques

National Cybersecurity Strategy (NCS)

- National Cybersecurity assessment
- NCS development support

In-Country Technical Assistance

- Technical Support (e.g. vulnerability assessments)
- Risk Management Support

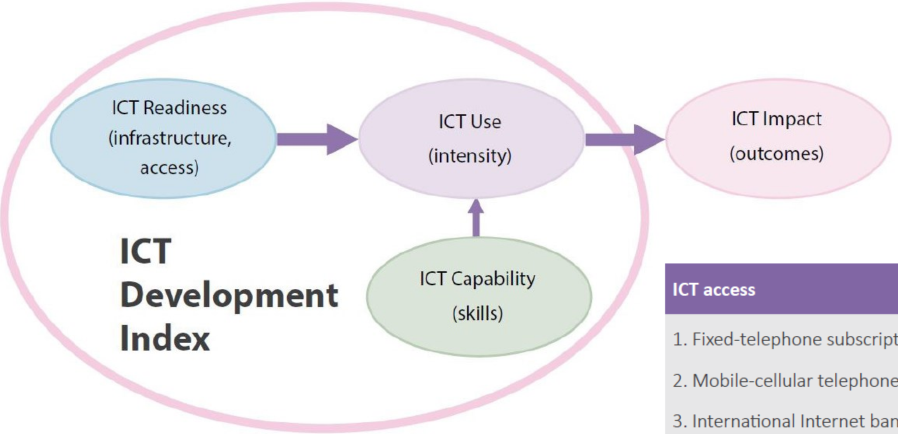
Human Capacity Building

- Curricula and Training Programs
- Bespoke Training

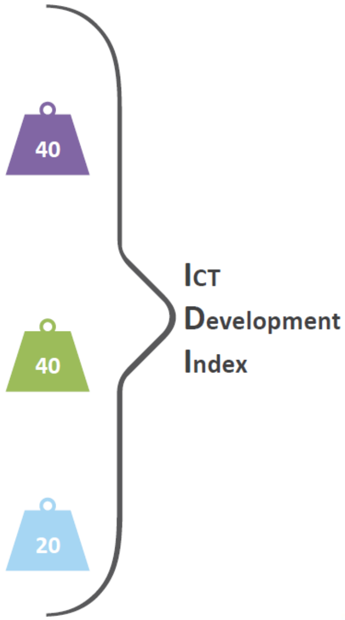
MIS – MEASURING THE INFORMATION SOCIETY REPORT

IDI – ICT DEVELOPMENT INDEX

Three stages in the evolution towards an information society

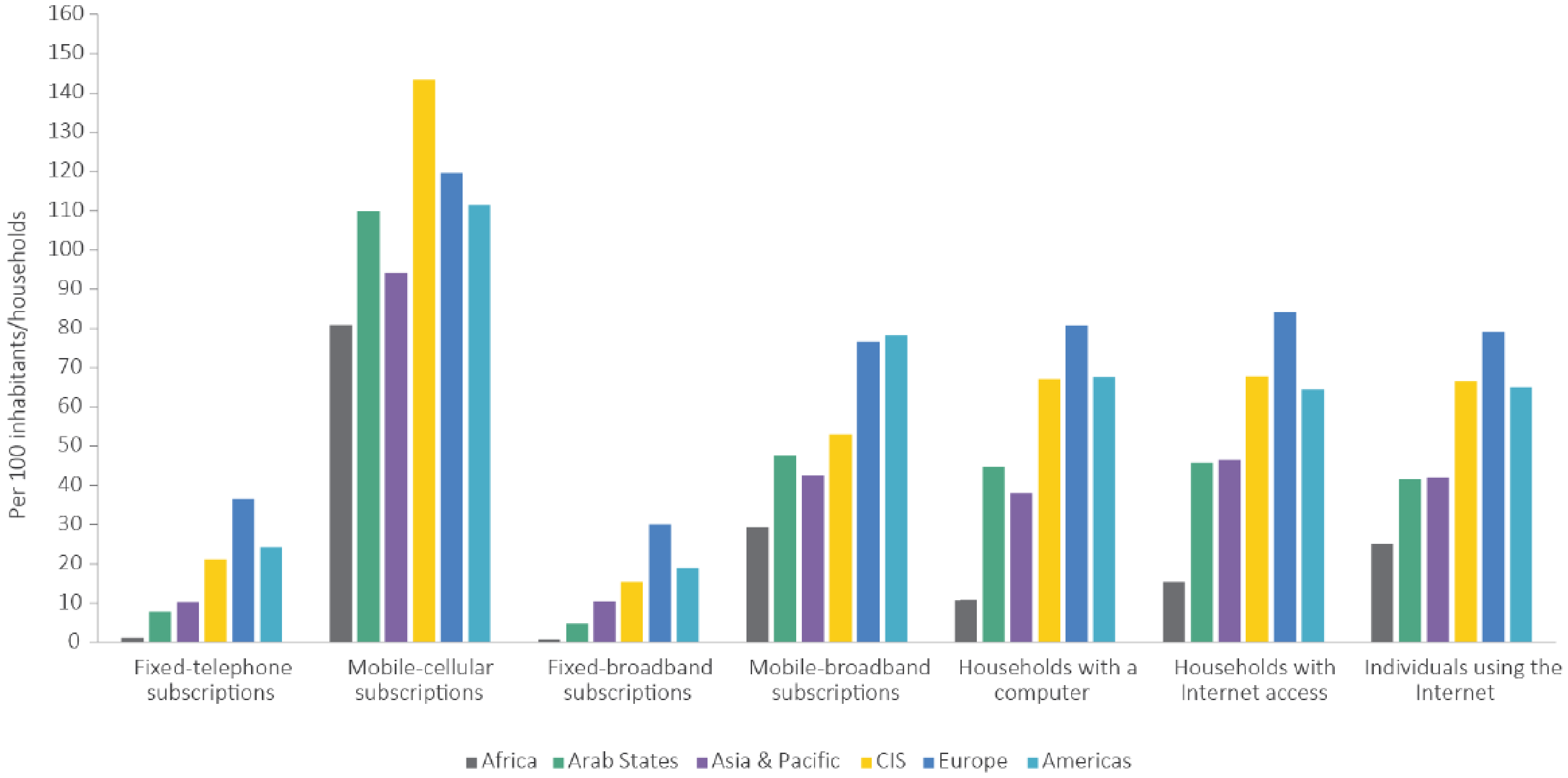


ICT access	Reference value	(%)
1. Fixed-telephone subscriptions per 100 inhabitants	60	20
2. Mobile-cellular telephone subscriptions per 100 inhabitants	120	20
3. International Internet bandwith (bit/s) per internet user	976’696*	20
4. Percentage of households with a computer	100	20
5. Percentage of households with Internet access	100	20
ICT use	**Reference value**	**(%)**
6.Percentage of individuals using the Internet	100	33
7. Fixed-broadband subscriptions per 100 inhabitants	60	33
8. Active mobile-broadband subscriptions per 100 inhabitants	100	33
ICT skills	**Reference value**	**(%)**
9. Mean years of schooling	15	33
10. Secondary gross enrolment ratio	100	33
11. Tertiary gross enrolment ratio	100	33



MIS – MEASURING THE INFORMATION SOCIETY REPORT

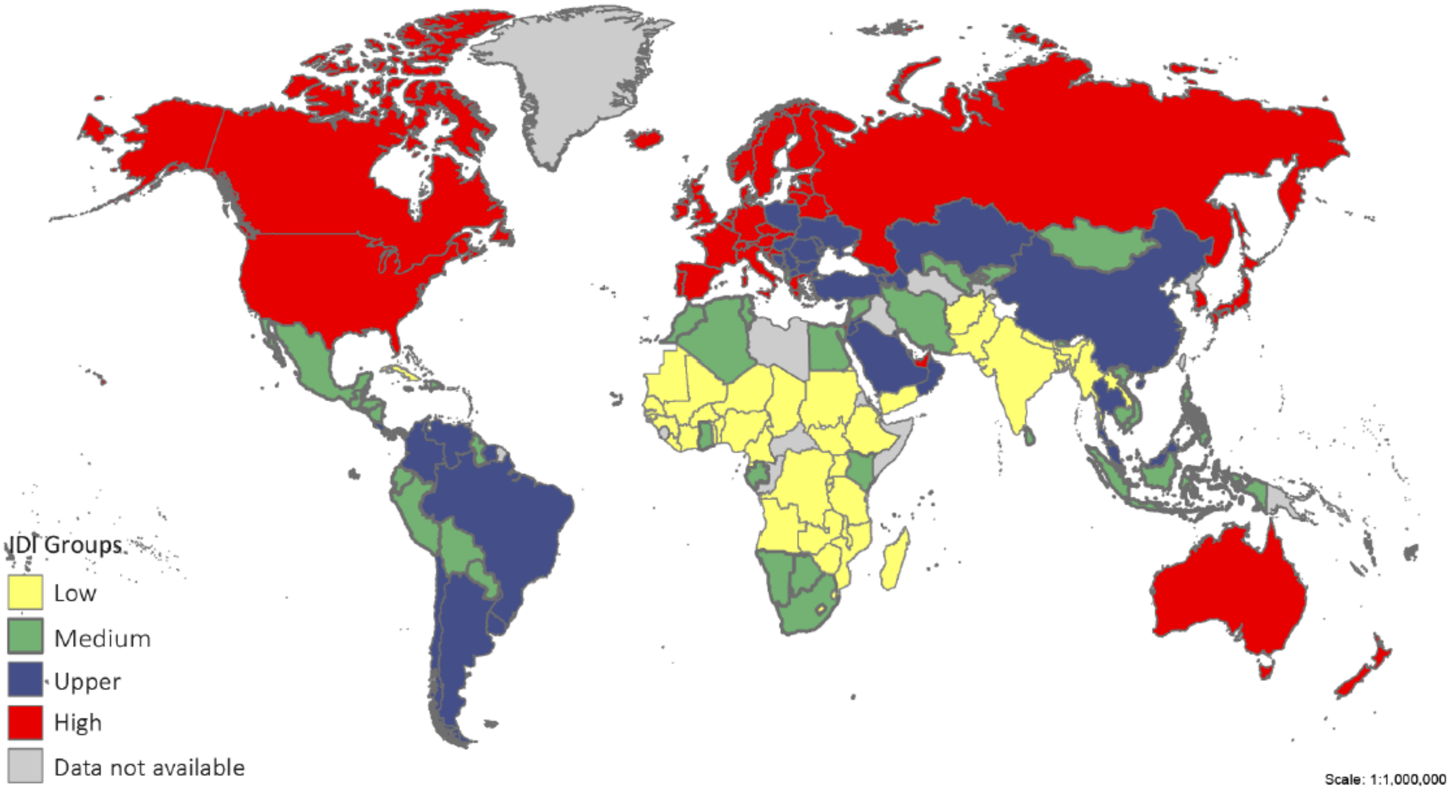
ICT penetration levels, 2016*, by geographic region



MIS – MEASURING THE INFORMATION SOCIETY REPORT

IDI – ICT DEVELOPMENT INDEX

Geographical distribution of IDI quartiles, 2016



Global Cybersecurity index - GCI

The GCI measures the commitment of countries to cybersecurity in the 5 pillars of the Global Cybersecurity Agenda:

- Legal Measures
- Technical Measures
- Organizational Measures
- Capacity Building
- Cooperation

Goals

- help countries identify areas for improvement
- motivate them to take action to improve their GCI ranking
- help harmonize practices
- foster a global culture of cybersecurity

Final Global and Regional Results are **on ITU Website**
http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

Global Cybersecurity index - Partnership

GCI PARTNERS for data sharing, response collection and expertise in analysis

FIRST
Improving Security Together

unicri
United Nations
Interregional Crime and Justice
Research Institute

KISA
Korea Internet & Security Agency

INDIANA UNIVERSITY

ACTIONABLE THREAT INTELLIGENCE
RED TEAM CYBER

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE

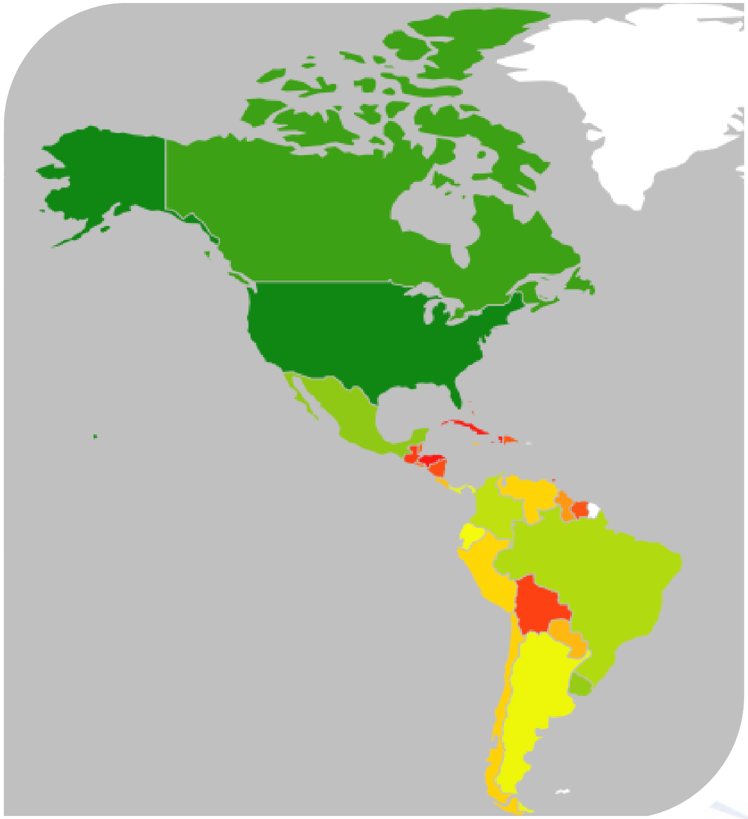
POTOMAC INSTITUTE FOR POLICY STUDIES

RCC
المركز العربي الإقليمي للأمن السيبراني
ITU - ARAB REGIONAL CYBERSECURITY CENTER

NTRA
EGYPT
National Telecom Regulatory Authority

WORLD BANK GROUP

Map of National Cybersecurity Commitments



National Cybersecurity Strategies

- Policy document, Strategy document, Action Plan
- Process for review and enhancement
- Standalone document or embedded in other strategies …
- Actionable, Sustainable
- A public document or not …
- Currently over **72** countries have published National Cybersecurity Strategies
- The oldest was issued in 2004 and the latest in 2015..

Some repositories are

- ITU *http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx*
- ENISA *https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world*
- NATO CCDCOE *https://ccdcoe.org/strategies-policies.html*

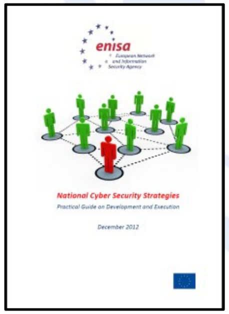
Source: ITU

National Cybersecurity Strategies - HOW

- Have a champion leading the work and ensuring that deliverable will move into implementation phase
- Set up a dedicated local team with the relevant representation and expertise
- Contract Consultancy / Expert services / bi-laterals with nations having expertise in NCS elaboration
- Use existing models, tools and resources
- Identify the appropriate information resources … how do nations do that ??
- Let's reduce the Confusion & Overlaps and create effective SYNERGIES

ITU NATIONAL CYBERSECURITY STRATEGY GUIDE

2011

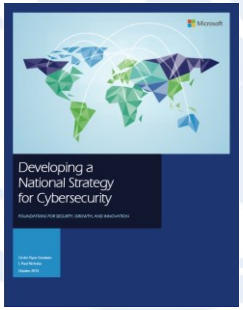

enisa
European Network and Information Security Agency

National Cyber Security Strategies

Practical Guide on Development and Execution

December 2012

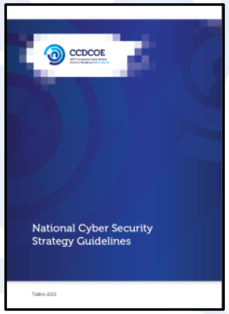
2012


Microsoft

Developing a National Strategy for Cybersecurity

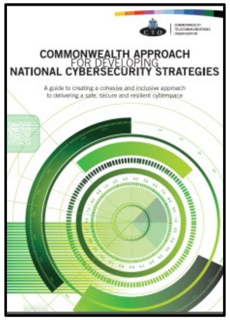
FOUNDATIONS FOR SECURITY, GROWTH, AND INNOVATION

2013


CCDCOE

National Cyber Security Strategy Guidelines

2013


COMMONWEALTH APPROACH FOR DEVELOPING NATIONAL CYBERSECURITY STRATEGIES

A guide to creating a cohesive and inclusive approach to delivering a safe, secure and resilient cyberspace

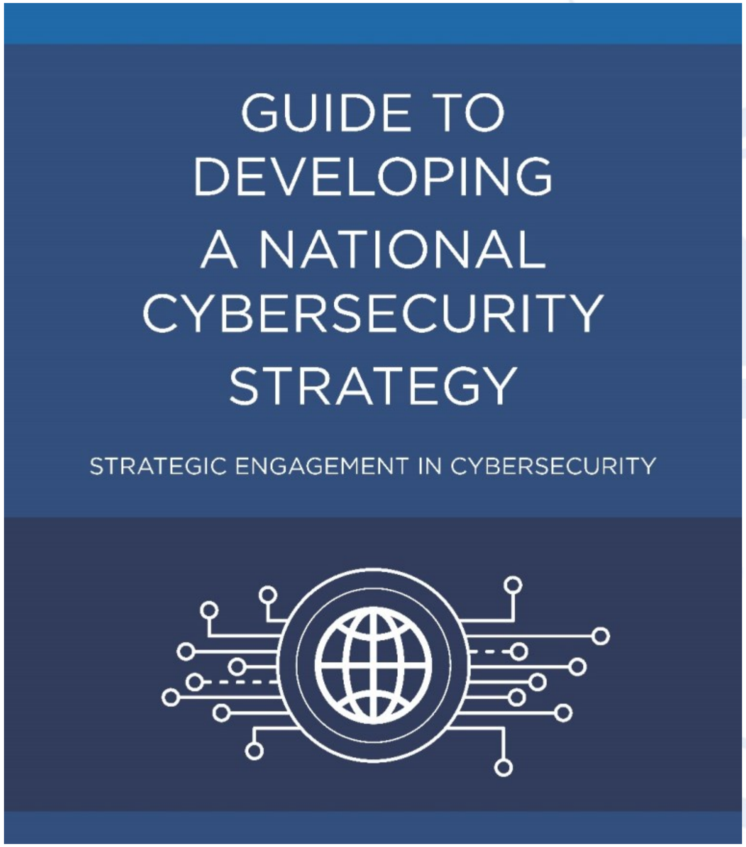
2014

And there are more great resources…

National Cyber Security Toolkit
Joint Effort by 15 Partners

UNITED NATIONS
UNCTAD
GCSP
RAND CORPORATION
THE WORLD BANK
IBRD · IDA | WORLD BANK GROUP
Organization of American States
ENISA
POTOMAC INSTITUTE FOR POLICY STUDIES
ITU
INTELLIUM
CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
OECD
BETTER POLICIES FOR BETTER LIVES
Microsoft
CTO
The Commonwealth Cybercrime Initiative
Global Cyber Security Capacity Centre

All project partners contribute their knowledge and expertise in the National Cyber Security domain



GUIDE TO DEVELOPING A NATIONAL CYBERSECURITY STRATEGY

STRATEGIC ENGAGEMENT IN CYBERSECURITY

The Commonwealth Cybercrime Initiative

CCDCOE

CTO

Global Cyber Security Capacity Centre

Deloitte.

GCSP
Geneva Centre for Security Policy
Where knowledge meets experience

ITU

Microsoft

POTOMAC INSTITUTE FOR POLICY STUDIES

UNITED NATIONS
UNCTAD

RAND
CORPORATION

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

Purpose

Guides national leaders and policy-makers in the development of a National Cybersecurity Strategy.

A unique resource. A framework agreed on by organisations with demonstrated and diverse experience in the topic and builds on their prior work in this space.

Scope

Focuses on protecting civilian aspects of cyberspace. Does not cover aspects related to developing offensive and defensive capabilities.

Provides indications on "what" should be included in a National Cybersecurity Strategy, as well as on "how" to build, implement and review it.

Lifecycle of a National Cybersecurity Strategy

Initiation

Implementation

Production of a national strategy

Stocktaking and analysis

Monitoring and evaluation

NCS Good Practice – Focus Areas

Focus Areas 1 - Governance

Focus Area 2 - Risk management in national cybersecurity

Focus Area 3 - Preparedness and resilience

Focus Area 4 - Critical infrastructure services and essential services

Focus Area 5 - Capability and capacity building and awareness raising

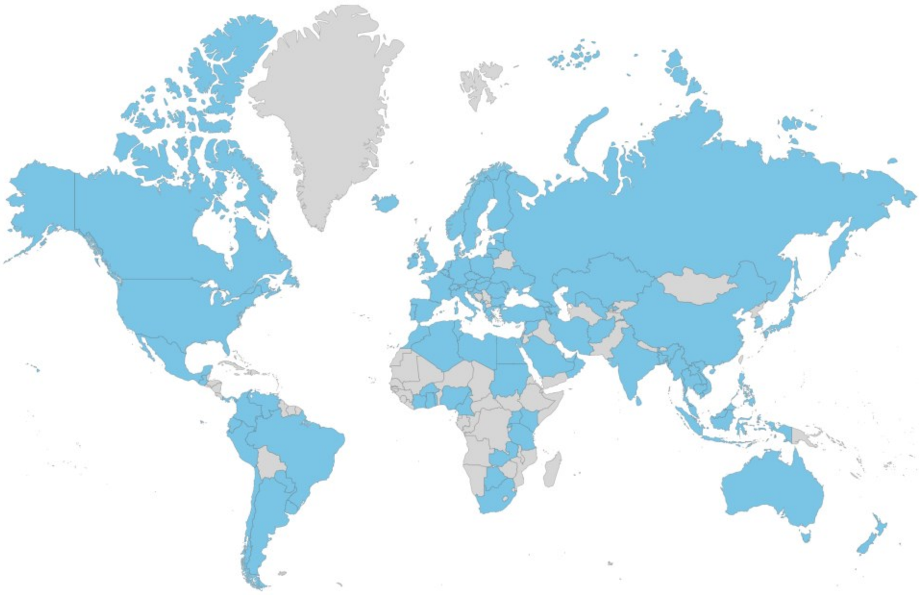
Focus Area 6 - Legislation and regulation

Focus Area 7 - International cooperation

National CIRTs
The First Line of Cyber-Response

Responsible for:

- Coordinating incident response
- Dissemination of early warnings and alerts
- Facilitating communications and information sharing among stakeholders
- Developing mitigation and response strategies
- Publishing best practices in incident response as well as prevention advice;
- Coordinating international cooperation on cyber incidents;



102 National CIRTs Worldwide
Need to fill the gap!

ITU’s National CIRT Programme

- Assessments conducted for **72** countries
- Implementation completed for **12** countries

  Barbados, Burkina Faso, Côte d'Ivoire, Cyprus (GOV CIRT), Ghana, Jamaica, Kenya, Montenegro, Tanzania, Trinidad and Tobago, Uganda, Zambia.

- Implementation in progress for **3** countries

  Burundi, Gambia, Cyprus (National CIRT)

- CIRT Enhancement in progress for 1 country

  Kenya

- **20 regional** cyber drills conducted with participation of over **100** countries

Computer Security Incident

“Any real or suspected adverse event in relation to the security of computer system or computer networks”.

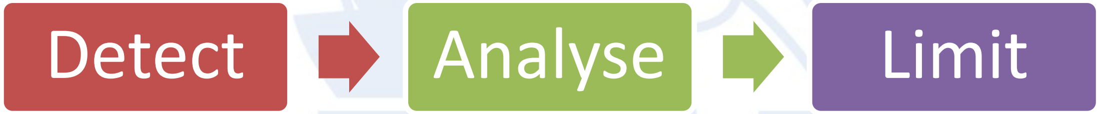
- (According to ‘CIRT FAQ’) in CERT/CC

A single or a series of unwanted or unexpected computer security events that have a significant probability of compromising business operations and threatening cybersecurity.

- ISO Definition

Incident response

Process of addressing computer security incidents


Detect

Analyse

Limit

Observe system for unexpected behaviour or anything suspicious

Investigate anything considered unusual.

If the investigation finds something that isn’t explained by authorized activity, immediately initiate response procedures.

Policies and procedures

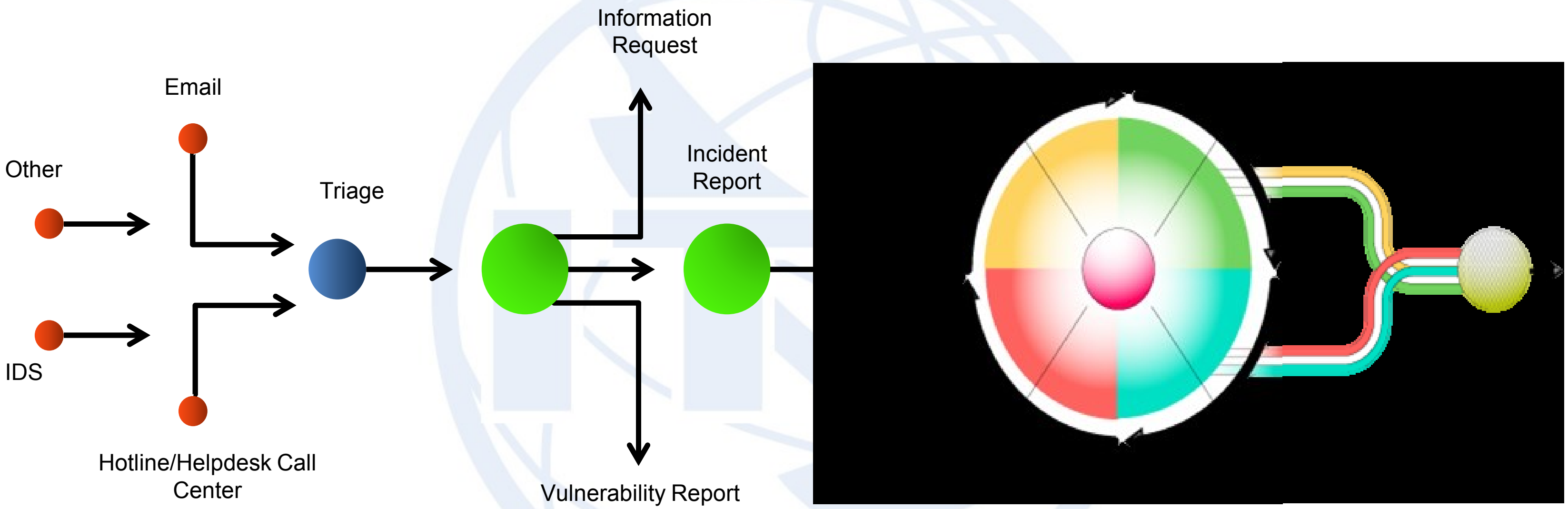
Established procedures must be in place to:

- Detect & identify the attack
- Mitigate the damage
- Recover from the attack

Without a formal process in place critical information may be lost

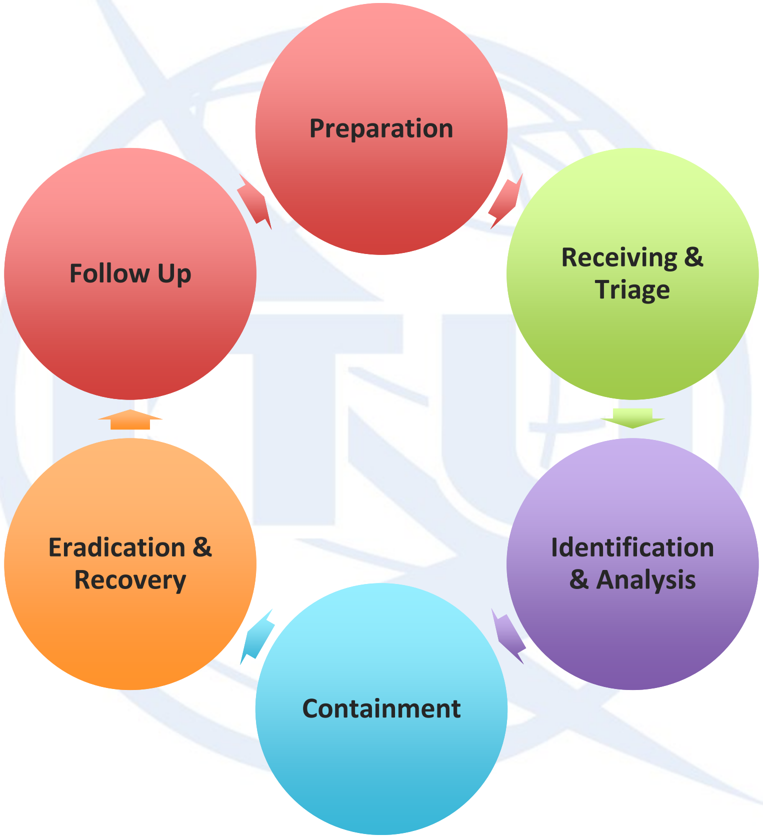
These procedures used in incident response can be thought of as the incident handling life cycle.

Incident handling life cycle

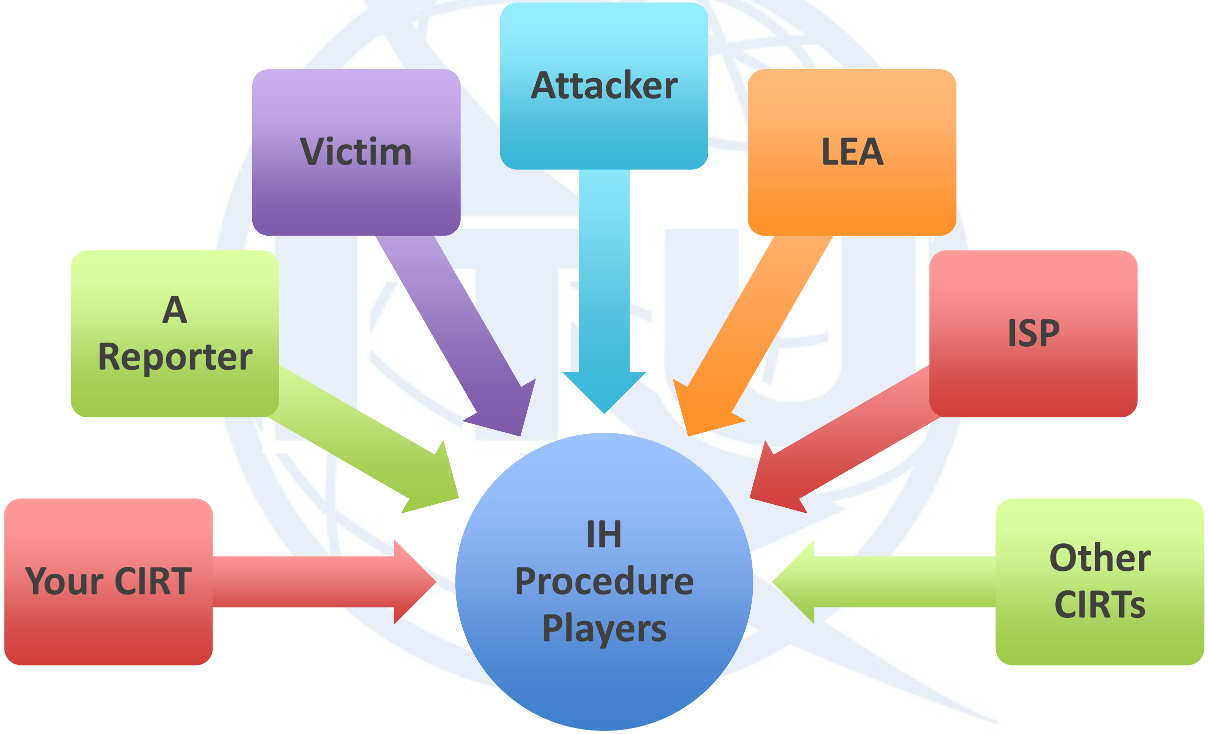


Source: CERT/CC Incident Handling Life Cycle in CERT/CC "Handbook for Computer Incident Response Teams (CIRTs)

Incident handling
Lifecycle in a CIRT perspective



Incident handling
Players involved



Incident handling
Typical format and required information

Contact Info

- Name
- Organization Name
- Division
- E-mail address or FAX number

Purpose of Reporting

- Question
- Information providing
- Request to coordination
- Other

Summary of the Incident

Source IP address or hostname
Description about the incident
System information of the system
IP address or hostname
Protocol / Port number
Hardware / OS
Timestamp
Time zone

Log Information

Incident handling
Triage – prioritizing incidents

High

- Urgent report like phishing
- Incident still active
- Have to coordinate to other organization

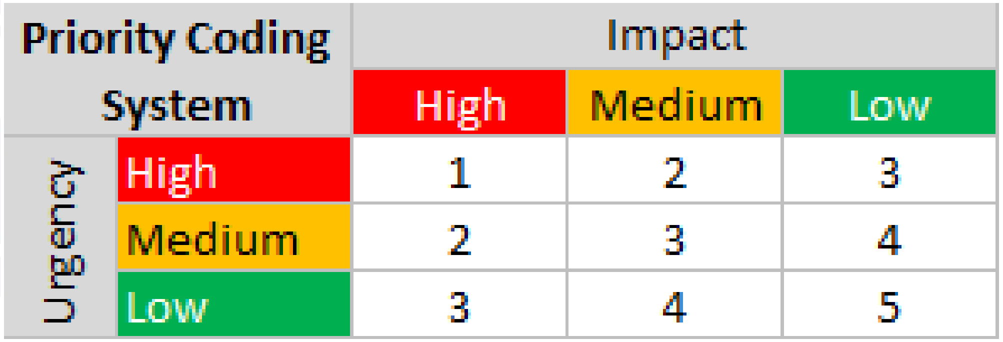
Middle

- Not urgent report
- Not active incident
- Will coordinate to other organization

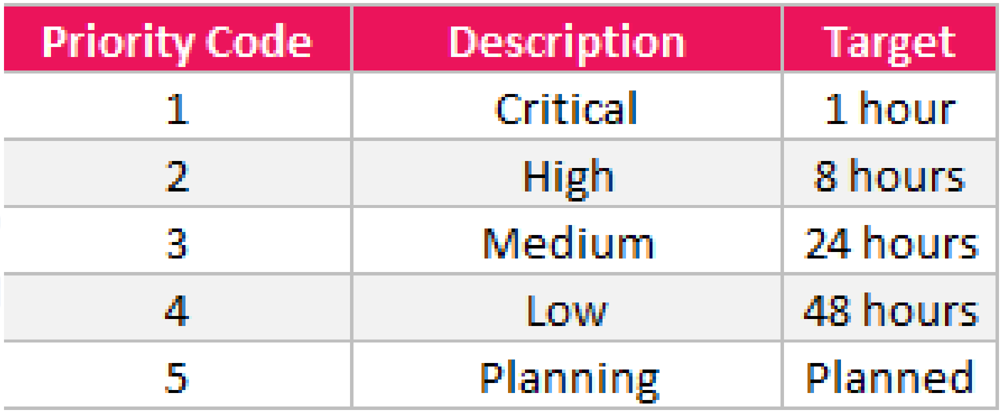
Low

- Just a technical question to answer
- Just a FYI to us

Others



Priority Coding System		Impact		
		High	Medium	Low
Urgency	High	1	2	3
	Medium	2	3	4
	Low	3	4	5



Priority Code	Description	Target
1	Critical	1 hour
2	High	8 hours
3	Medium	24 hours
4	Low	48 hours
5	Planning	Planned

Incident handling
Identification and analysis

Define objectives and investigate situation

- Who has attacked us?
- What is the scope and extent of the attack?
- When did the attack occur?
- What did the attackers take from us?
- Why did they do it?

Determine what investigation actions are to be taken.

Determine CSIRT resources are required to conduct the investigation, request/secure hardware, software, personnel resources.

Communicate with parties that need to be aware of the investigation.

Incident handling Containment

- Take appropriate action to contain the incident.
  - Blocking (and logging) of unauthorised access.
  - Blocking malware sources (e.g. email addresses and websites).
  - Blocking botnet connections to external site.
  - Closing particular ports and services.
  - Changing system administrator passwords where compromise is suspected.
  - Firewall filtering.
  - Relocating website home pages.
  - Isolating systems.
- Delayed containment is usually NOT good.
- Need additional evidence to do containment?
- Need to get approval from legal section?
- If so (above), attacker could escalate unauthorized access / compromise other system in short time.
- Other potential issues.
- Some attacks may cause additional damage when contained (e.g. disconnected).

Incident handling - Documentation

Carry out a post incident review.

- Important information about the cyber security incident should be discussed during a post incident review.
- All key discussions and decisions conducted during the eradication event should be well documented.
- A report should be produced from the post incident review and presented to all relevant stakeholders.

Incident history: Chronicle of all email and other correspondence.

Status: Current status of the incident.

Actions: List of past, current, and future actions to be taken.

Incident coordinator: A team may choose to assign a staff member to coordinate the response to this incident.

Quality assurance parameters: Information that might help to measure the quality of the service.

Incident handling - Communication

Report the incident to relevant stakeholders

- ❖ A full description of the nature of the incident, it’s history, and what actions were taken to recover
- ❖ A realistic estimate of the financial cost of the incident, as well as other impacts on the business
- ❖ Recommendations regarding enhanced or additional controls required to prevent, detect, remediate or recover from cyber security incidents more effectively

Communicate and build on lessons learned

- ❖ To document, communicate and build on lessons learned
- ❖ On-going process through which you can collaborate and learn from previous mistakes, incidents and experiences
- ❖ Develop an action plan to leverage on lessons learned to become more resilient in the face of future cyber security attacks

Incident handling - Self learning

Update key information, controls & documents

- Review security incident management methodologies or processes.
- Review management controls (e.g. training and awareness).
- Review Technical controls (e.g. patching, configuring system logs, and use of intrusion prevention/detection tools).
- Review Internal IT auditing procedures.
- Post-mortem after the incident is resolved.
- The meeting is helpful in improving security measures and the incident handling process itself.
- Assess time and resources used and damage incurred.
- Update policy and procedures as necessary.
- Update knowledgebase.

Regional Cyber Drills

- **2018 –Cybersecurity & CyberDrill – Argentina**
  - April, 2018, Argentina
  - Hosted by Universidad de la Plata and Ministry of Modernization
- **2017 – Caribbean Cybersecurity & CyberDrill - Suriname**
  - 3 to 7 July, 2017, Paramaribo - Surinam
  - Hosted by the Telecommunicatie Autoriteit Siriname
- **2017 – Americas Cybersecurity Regional Symposium**
  - 26 to 29 September, 2017, Montevideo - Uruguay
  - Hosted by AGESIC
- **2016 – Cybersecurity Week from the Center of the World and Fourth Cyberdrill for the America Region**
  - 27 June to 1 July 2016, Quito, Ecuador
  - Hosted by Ministry of Telecommunications and Information Society (MINTEL) and taking place at the University Politecnica Nacional
- **2015 – Regional Forum on Cyber security and Third Cyberdrill for the America Region**
  - 3 to 6 August 2015, Bogota, Colombia
  - Hosted by the Ministry of Information, Technology, and Communications of Colombia and The Colombian Chamber for Informatics and Telecommunications (CCTI) and taking place at the University of Los Andes
- **2014 – Applied Learning for Emergency Response Teams**
  - 8 to 10 September 2014, Lima, Peru
  - Co-organized with IMPACT at the invitation of INICTEL UNI
- **2013 – Applied Learning for Emergency Response Teams**
  - 26 to 28 August 2013, Montevideo, Uruguay
  - Co-organized with IMPACT, at the invitation of Latin American and Caribbean Internet Addresses Registry (LACNIC)

THANK YOU VERY MUCH!!!

QUESTIONS?

SDGs: ICT for Sustainable Development

- SDG 1: No Poverty
- SDG 2: Zero Hunger
- SDG 3: Good Health and Well-being
- SDG 4: Quality Education
- SDG 5: Gender Equality
- SDG 6: Clean Water and Sanitation
- SDG 7: Affordable and Clean Energy
- SDG 8: Decent Work and Economic Growth
- SDG 9: Industry, Innovation and Infrastructure
- SDG 10: Reduced Inequalities
- SDG 11: Sustainable Cities and Communities
- SDG 12: Responsible Consumption and Production
- SDG 13: Climate Action
- SDG 14: Life Below Water
- SDG 15: Life on Land
- SDG 16: Peace, Justice and Strong Institutions
- SDG 17: Partnerships for the Goals