TECHNOLOGICAL TENDENCIES IN DIGITAL RISK

Bruno Ramos
Regional Director, ITU Regional Office for the Americas Region
International Telecommunications Union

ITU's Regional Offices

ITU's Structure

Radiocommunication
ITU-R

Coordinates global wireless communication

Standardization
ITU-T

Produces interoperable technical ICT standards

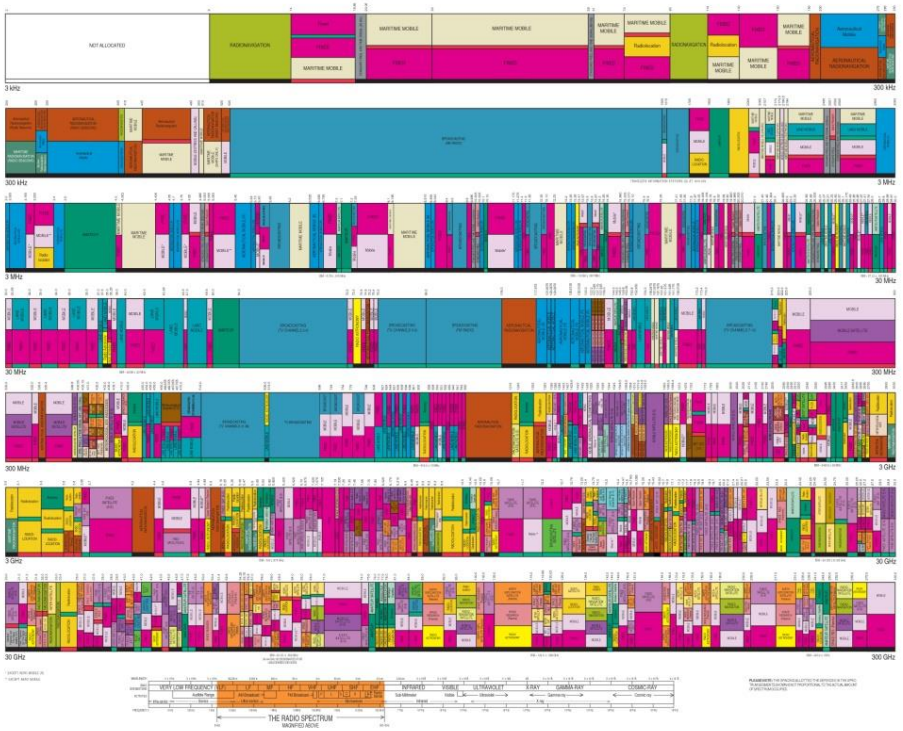
Development
ITU-D

Provides assistance to the un-connected

The General Secretariat provides intersectorial coordination for the whole organization

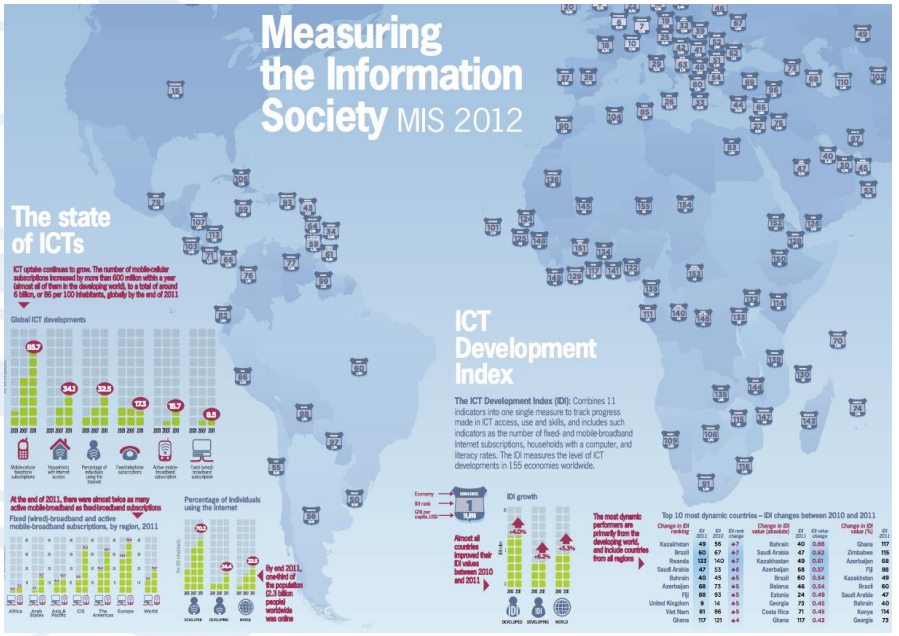
ITU-R: Radiocommunication Sector

Manages the radio-frequency spectrum and satellite orbits



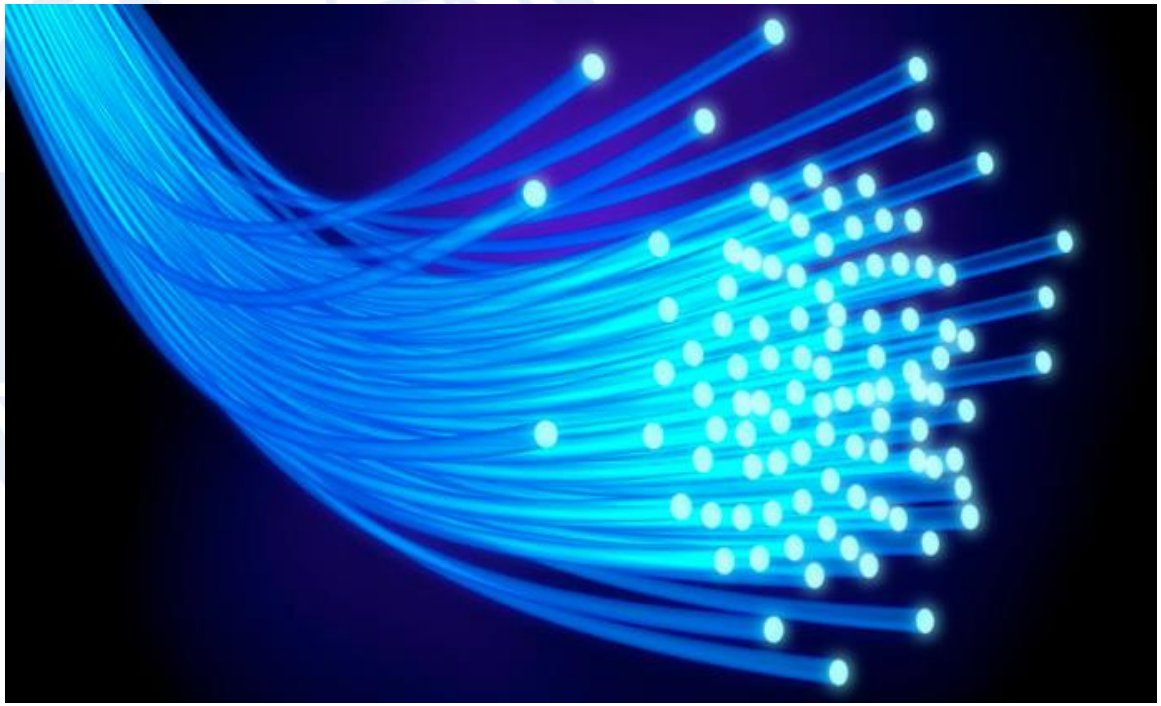
ITU-D: Development Sector

Assists the development of ICTs in the developing world



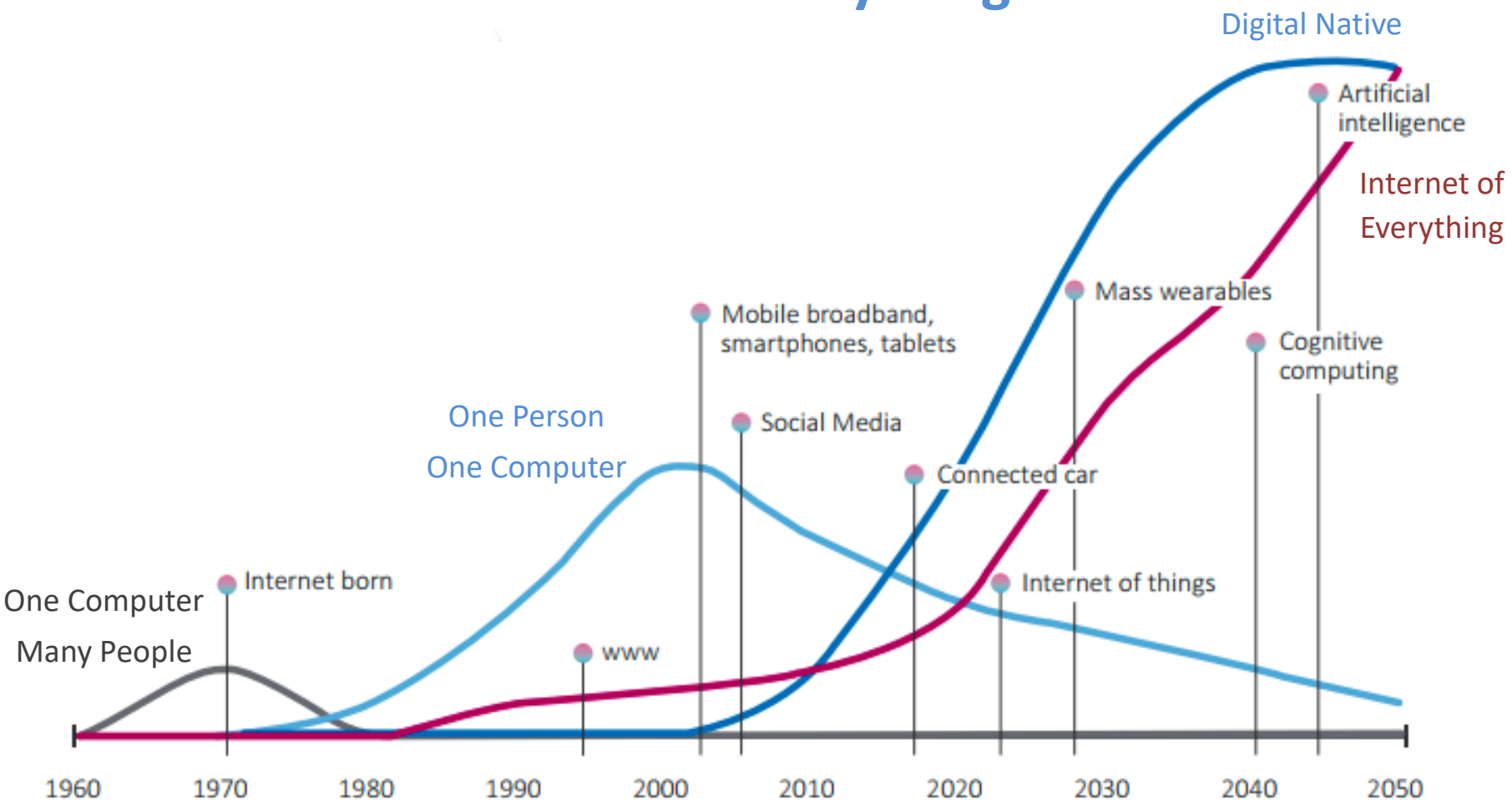
ITU-T: Standardization Sector

Produces standards covering all fields of telecommunications on a worldwide basis, and defines tariff and accounting principles for international telecommunication services



WHAT IS NEW?

Internet of Everything!!!



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

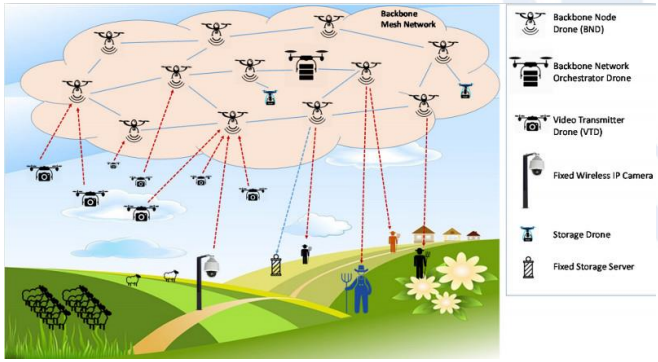
Everything is getting interconnected!!!

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

Artificial Intelligence / Robots
Autonomous Cars
Smart Homes / Smart Cities
Etc.

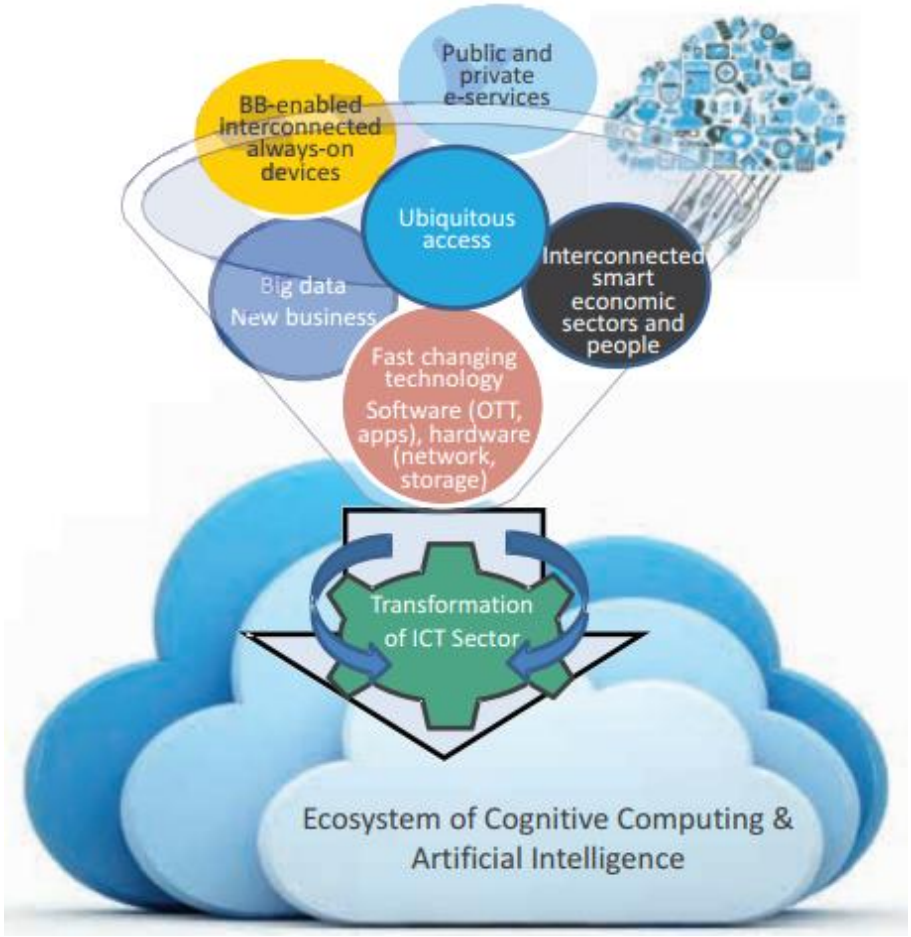
Increasing connections M2M
IoT – Internet of Everything
smarter sensors



Drones is its applications

5G networks / Smart Cities
Cloud Computing / Big Data

Digital Ecosystem



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

All Electronic Devices and Systems can Suffer Cyberattacks

Cell Phones / Laptops / Pads / PCs

Calculators / Cards / Cars / Sensors

Airplane / Drones / Industry

Home Management Systems

Systems at Hospitals

Country's Critical Infrastructure, etc.

IT IS HIGHLY IMPORTANT TO ADOPT CYBERSECURITY MEASUREMENTS!!!

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

=

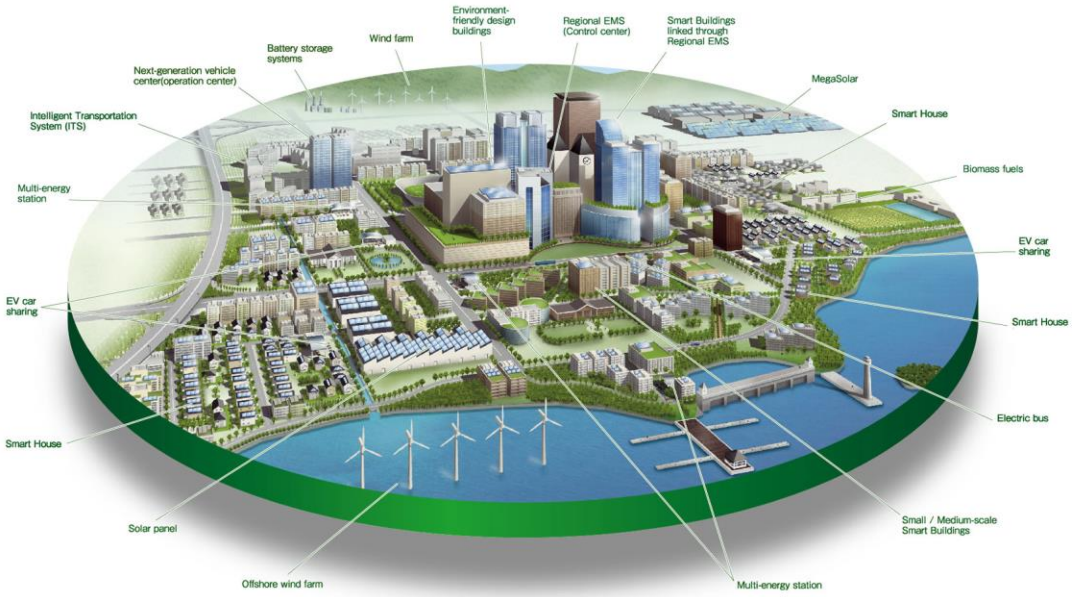
Hypervulnerability

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

Example: Smart Autonomous Car

ITU Magazine No2 2016 Building Smart and Sustainable Cities for tomorrow

What is considered as Critical Infrastructure?



Electrical System | Water System | Transportation

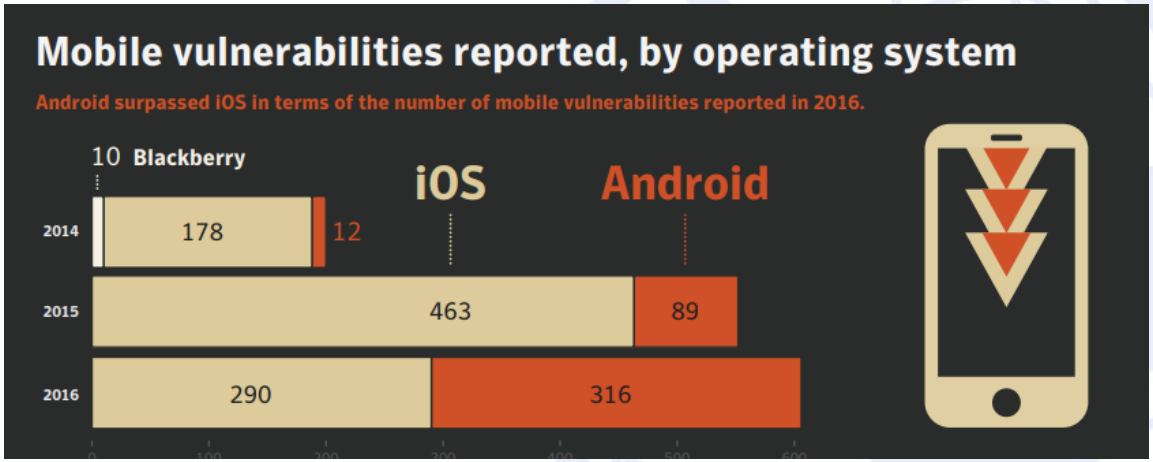
Gas System | Agriculture | Financial System

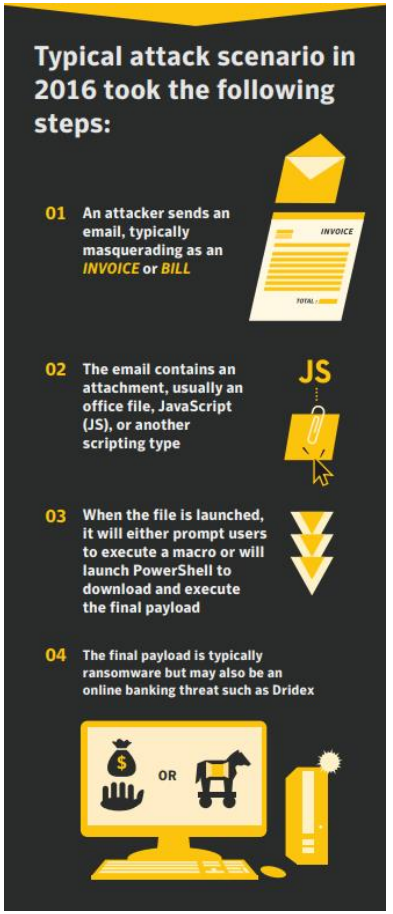
Oil System | Health | Police, Army, City Security

Industrial Sector | National Telecommunications Systems | Chemistry Sector

What are the Cyberthreats!!!

Some numbers of 2016





Symantec: Internet Security Threat Report, April 2017, Volume 22

Underground Market 2016

Symantec: Internet Security Threat Report, April 2017, Volume 22

Some numbers of 2016

Top 10 countries by number of data breaches

The United States was the country most heavily affected by data breaches in 2016

Rank	Country	Breaches
1	United States	1023
2	United Kingdom	38
3	Canada	19
4	Australia	15
5	India	8
6	Ireland	8
7	Japan	7
8	Israel	6
9	Germany	5
10	Thailand	5

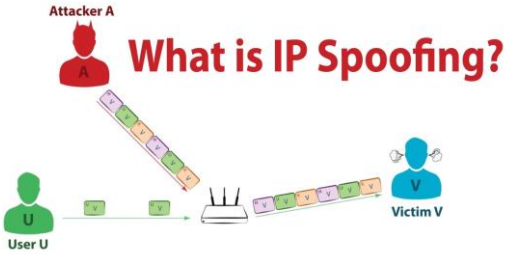
Top 10 sectors breached by number of incidents

Services was the industry most affected by data breaches in 2016.

Rank	Industry	Breaches	Percent
1	Services	452	44.2
2	Finance, Insurance, & Real Estate	226	22.1
3	Manufacturing	116	11.3
4	Retail Trade	84	8.2
5	Transportation & Public Utilities	75	7.3
6	Wholesale Trade	32	3.1
7	Construction	20	2.0
8	Mining	8	0.8
9	Public Administration	6	0.6
10	Nonclassifiable Establishments	3	0.3

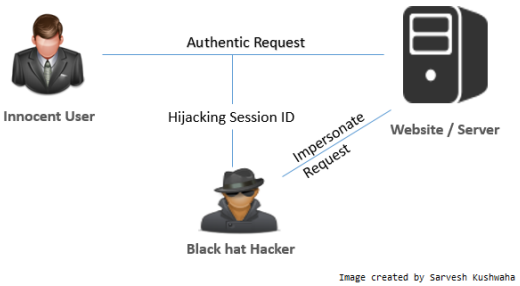
Symantec: Internet Security Threat Report, April 2017, Volume 22

CyberAttacks and Hacking

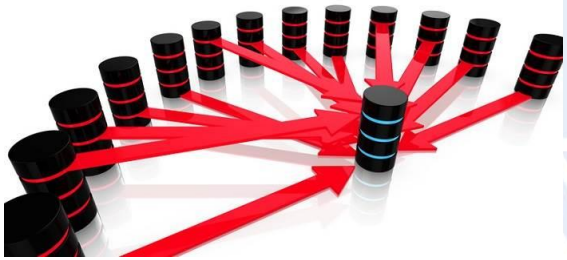


IP Spoofing

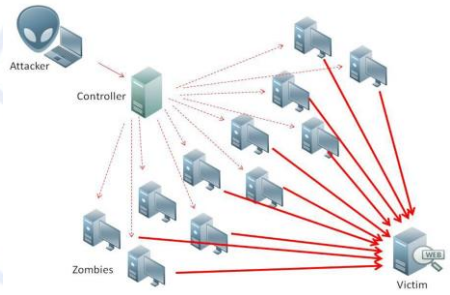
Fishing



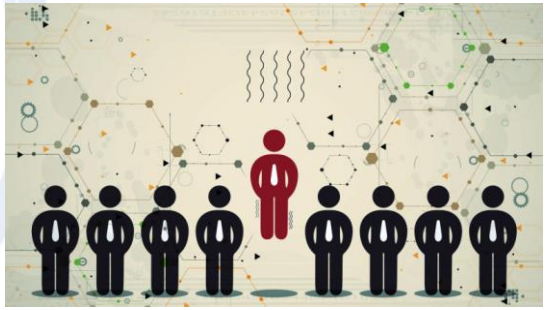
Session Hijacking
Man-in-the-Middle



DoS



DDoS, rDoS



Social Engineering

Ramsomeware
Virus

Exploits
Worms

SQL injection
Spyware

Credential Reuse
Spam

Threat Intelligence

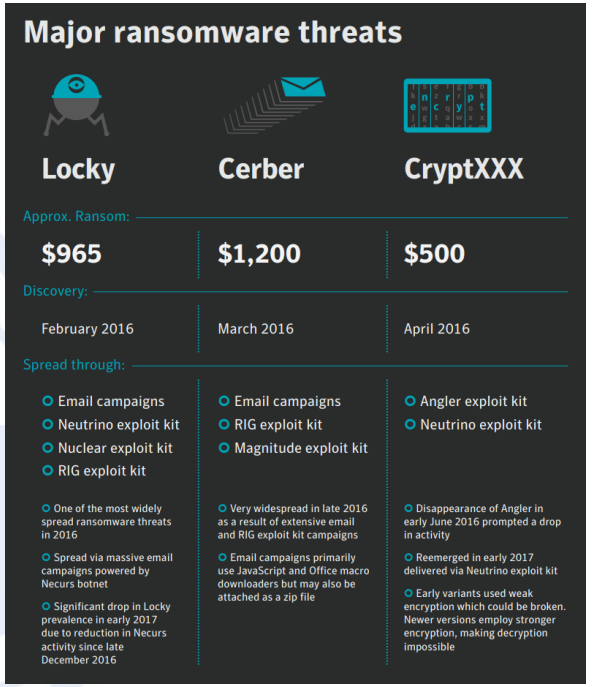
"Details of the motivations, intent, and capabilities of internal and external threat actors. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications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



"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." **

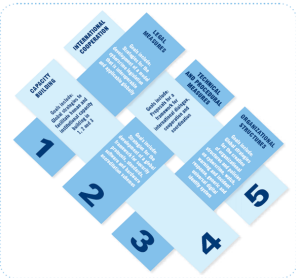
*TrendMicro: https://www.trendmicro.com/vinfo/us/security/definition/ransomware / ** Symantec: Internet Security Threat Report, April 2017, Volume 22

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



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.

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.

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

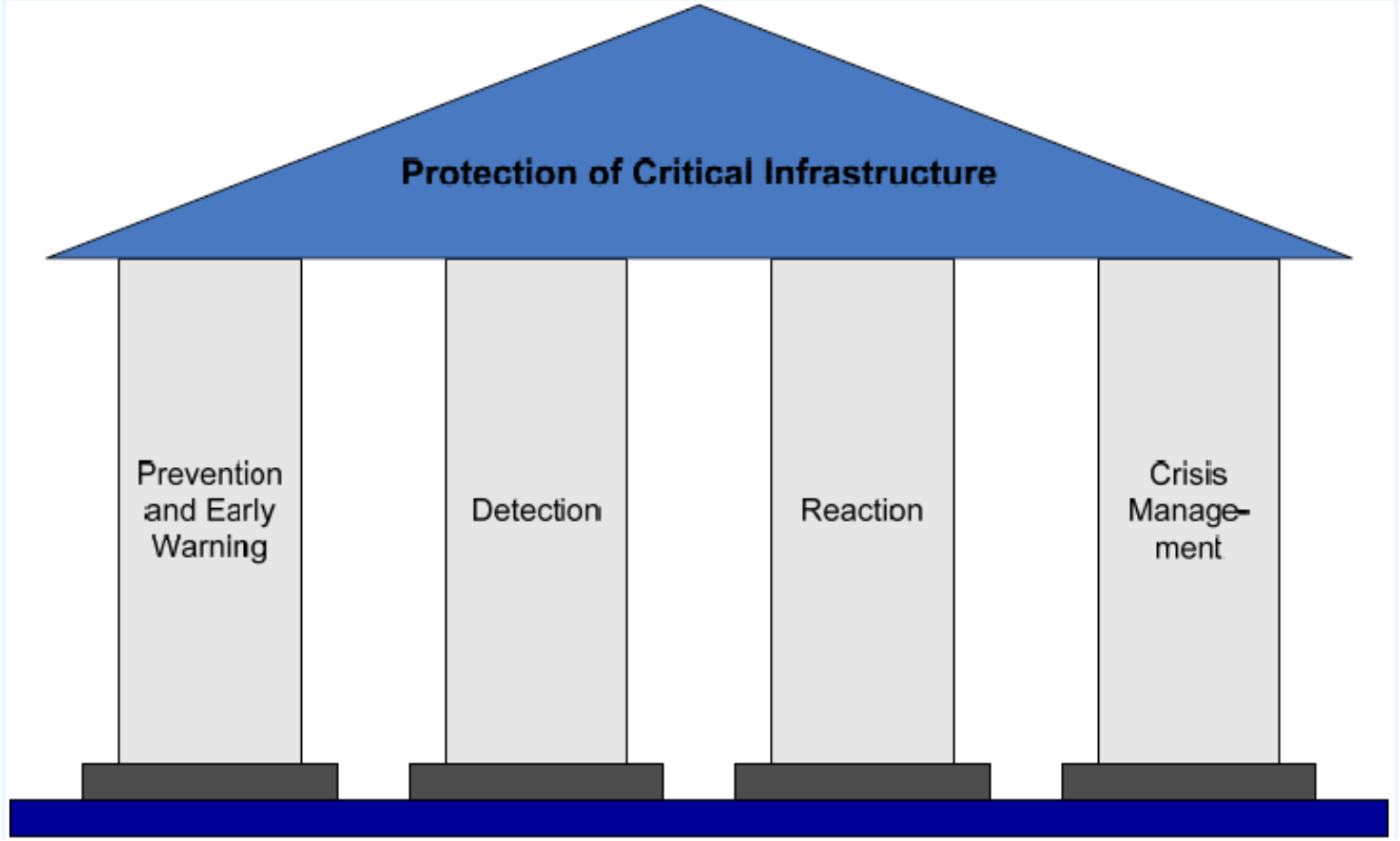
Net neutrality

Payments

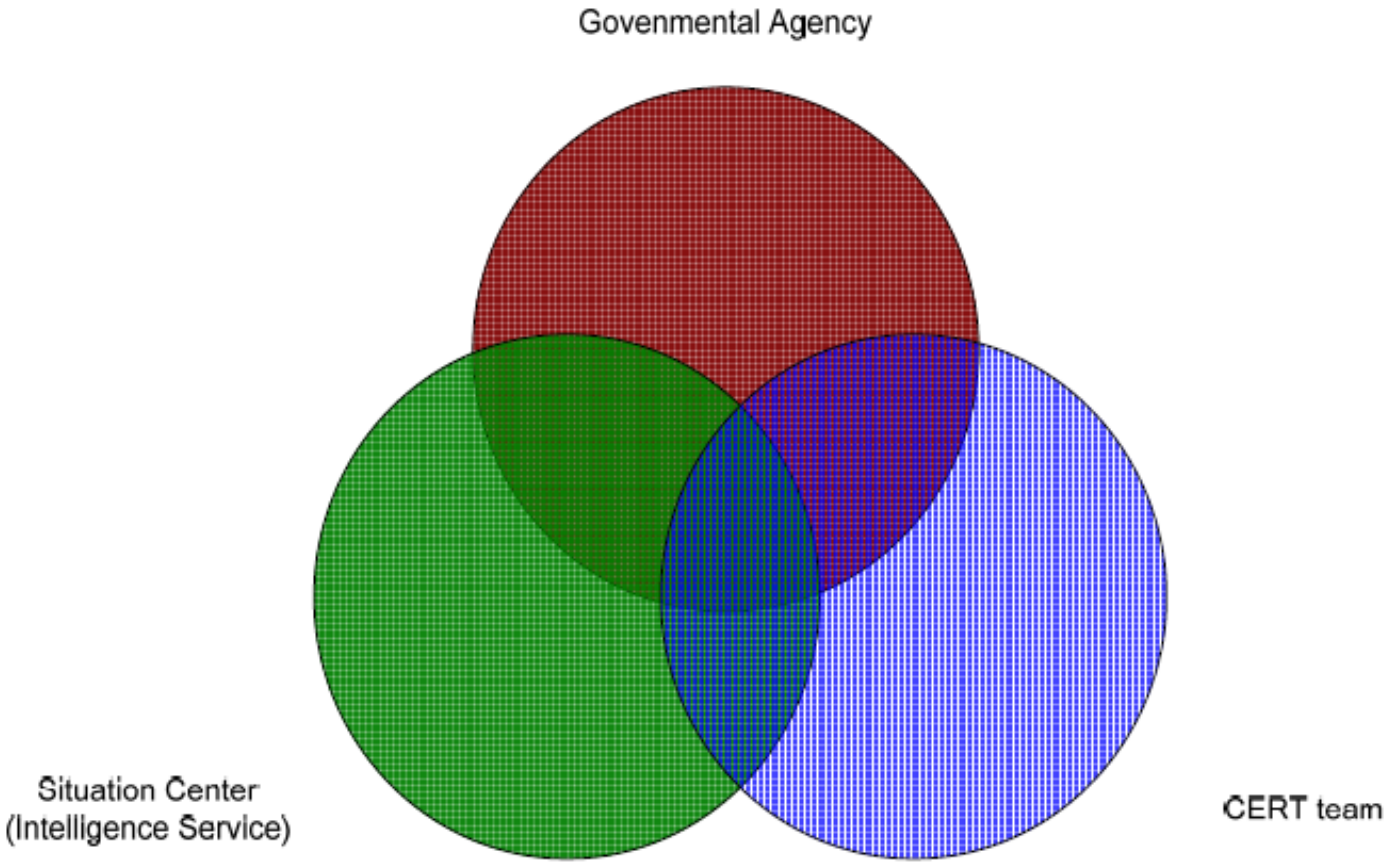
Consumer education

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

National Cybersecurity Strategy (NCS)

- National Cybersecurity assessment
- NCS development support

In-Country Technical Assistance

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

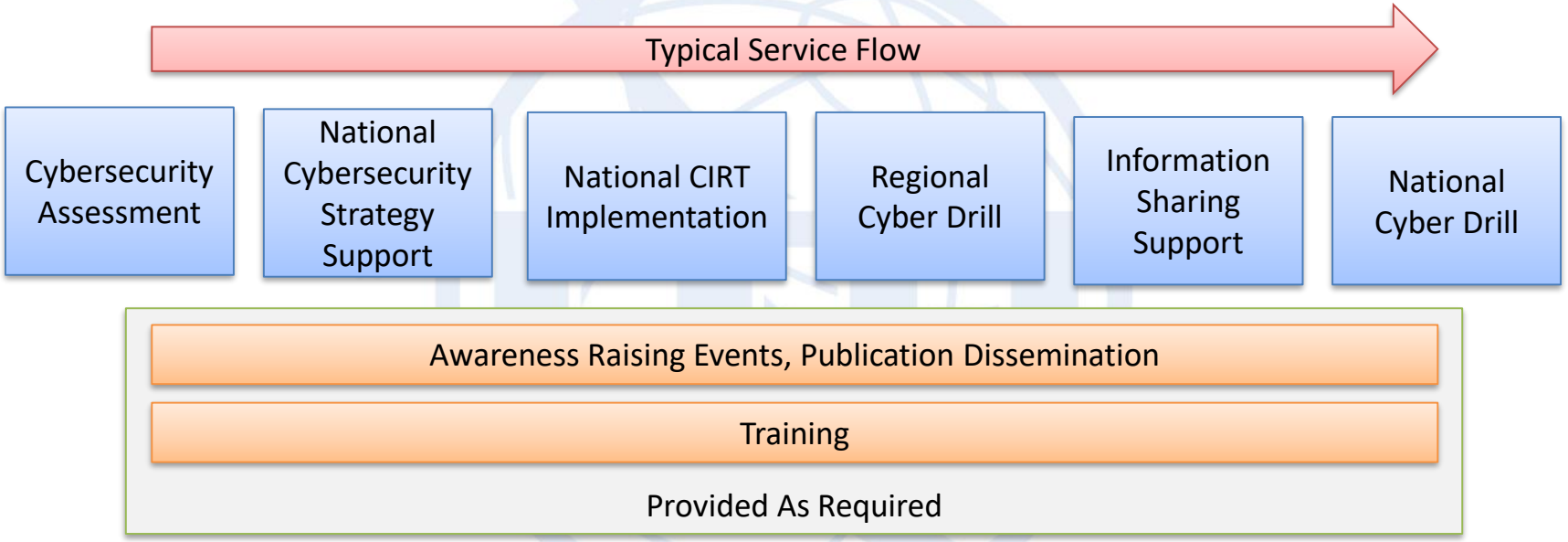
Information sharing

- Best Practices Sharing
- Information Exchange Tools and Techniques

Human Capacity Building

- Curricula and Training Programs
- Bespoke Training

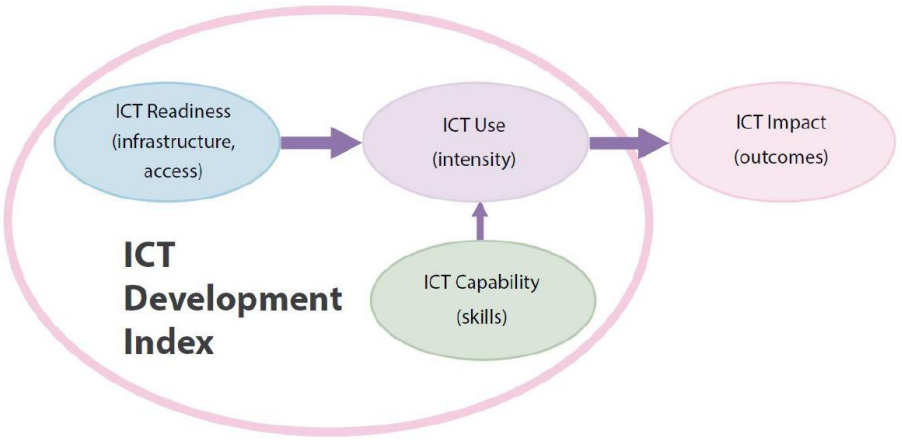
Flow of Cybersecurity Services



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

40

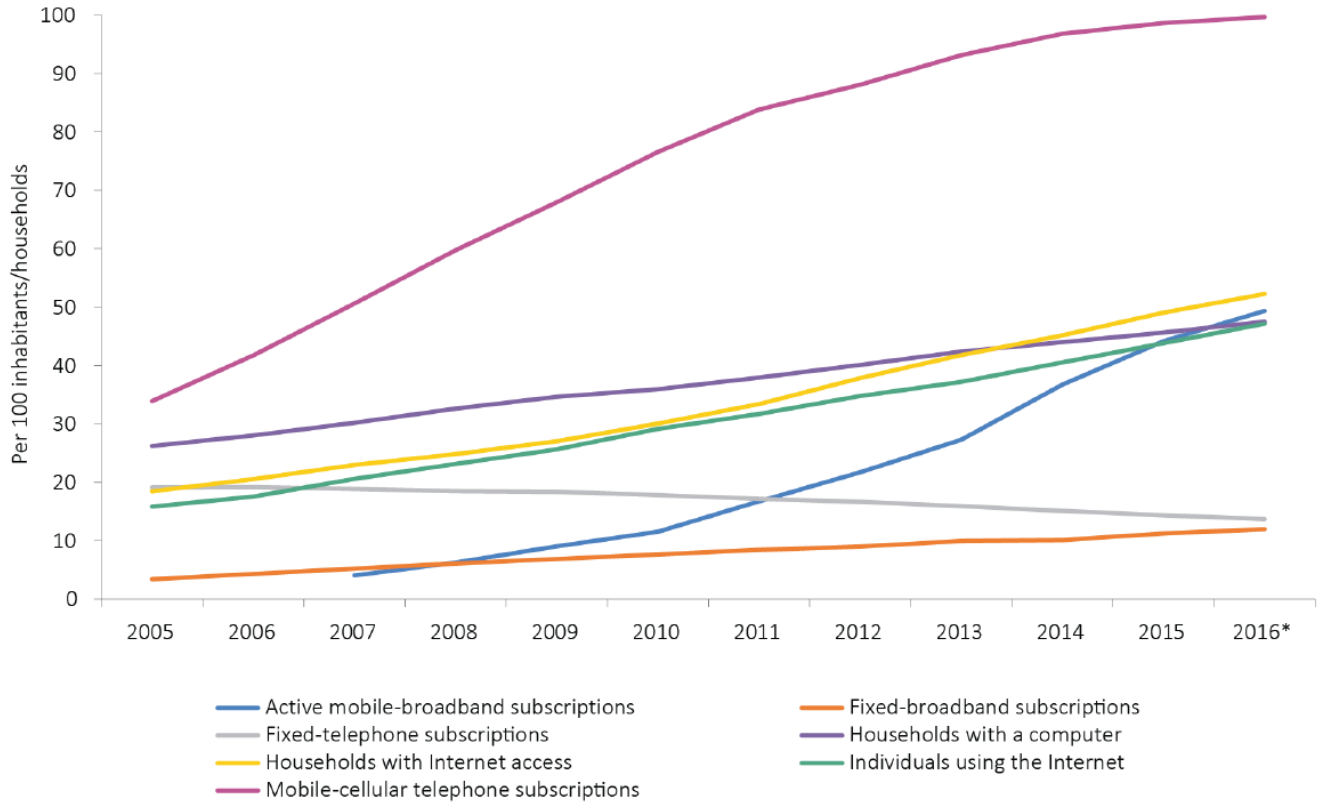
40

20

ICT Development Index

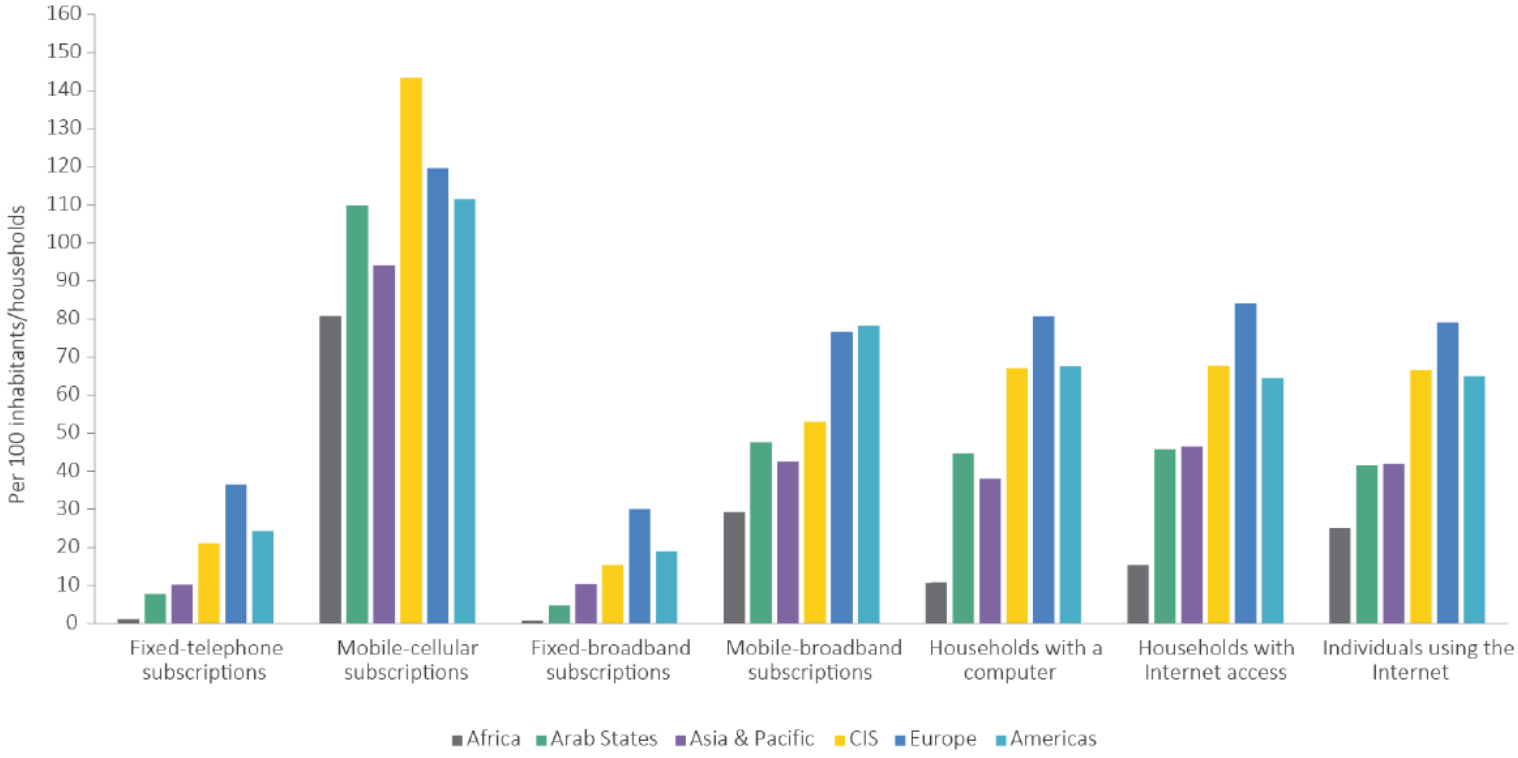
MIS – MEASURING THE INFORMATION SOCIETY REPORT

Global changes in levels of ICT uptake per 100 inhabitants, key ICT indicators, 2005-2016*



MIS – MEASURING THE INFORMATION SOCIETY REPORT

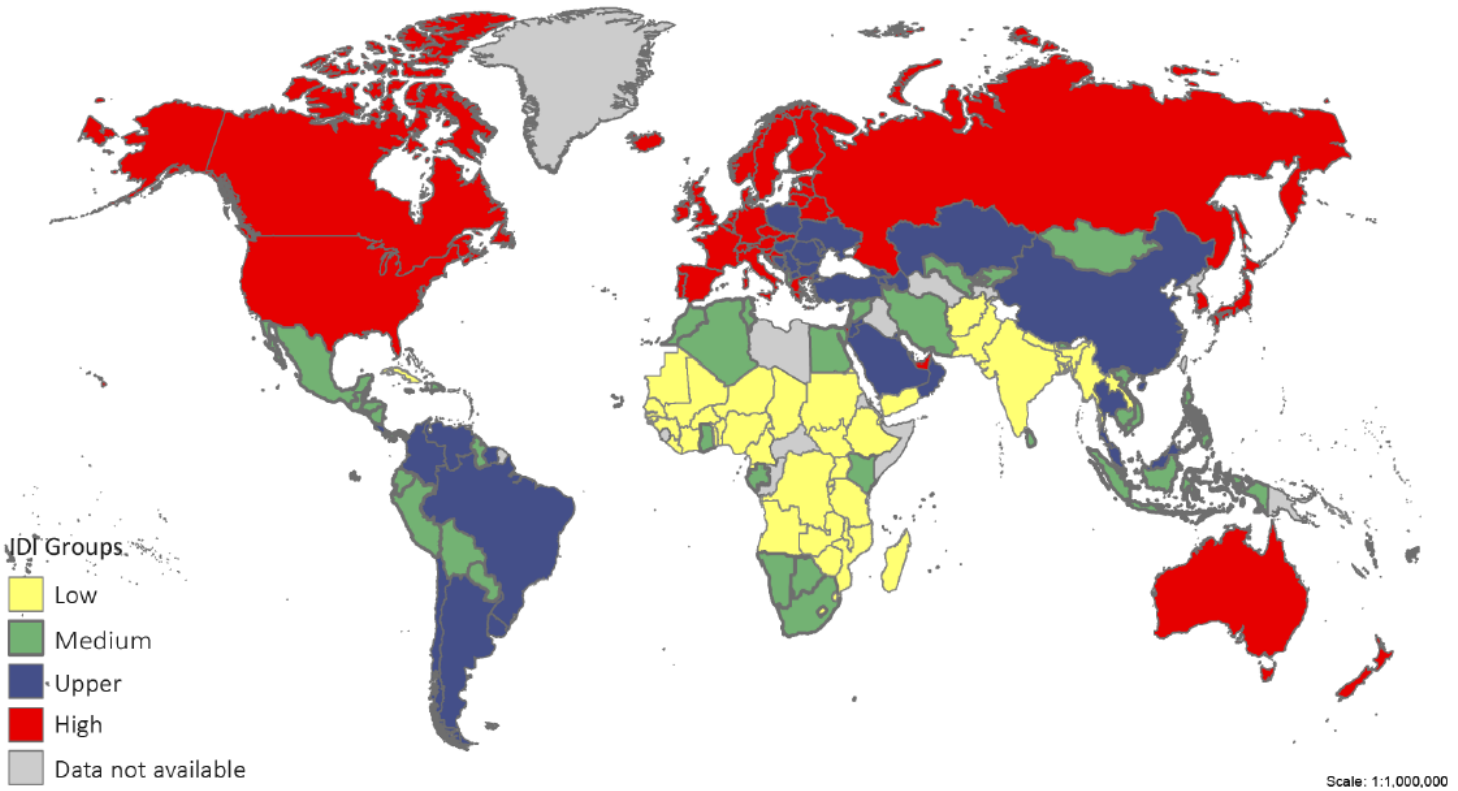
ICT penetration levels, 2016*, by geographic region



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

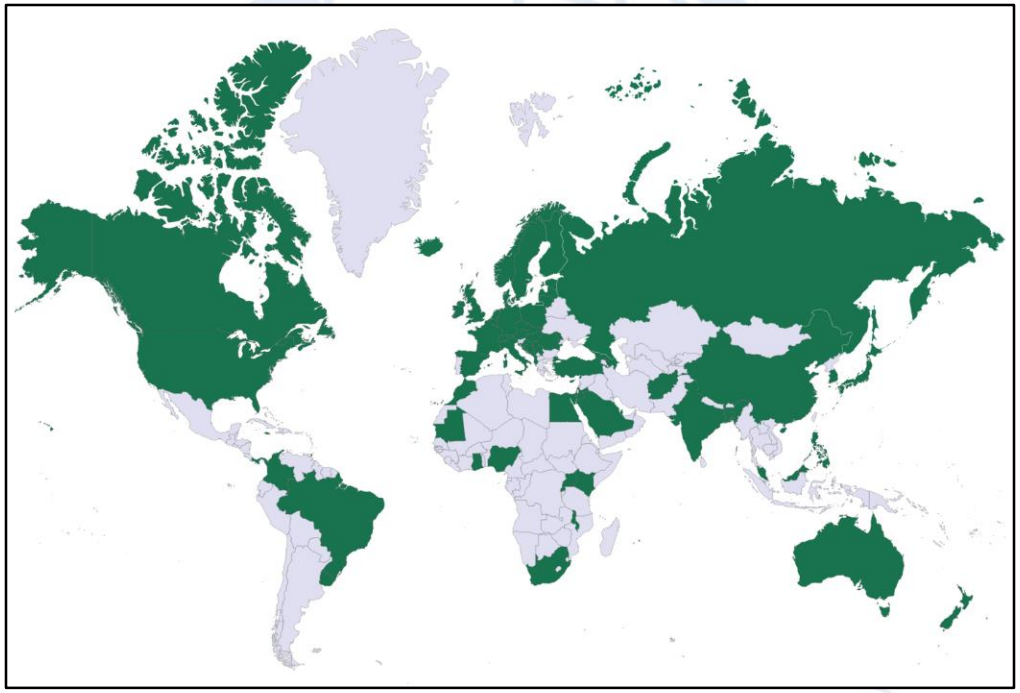
Goals

- 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

National Cybersecurity Strategy Guide

Reference Guide and Support Tool to help Member States produce a National Cybersecurity Strategy



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 67 countries
- Implementation completed for 11 countries

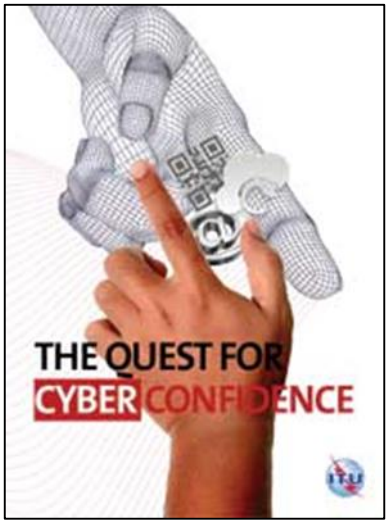
  Burkina Faso, Côte d'Ivoire, Cyprus, Ghana, Jamaica, Kenya, Montenegro, Tanzania, Trinidad and Tobago, Uganda, Zambia.
- Implementation in progress for 4 countries

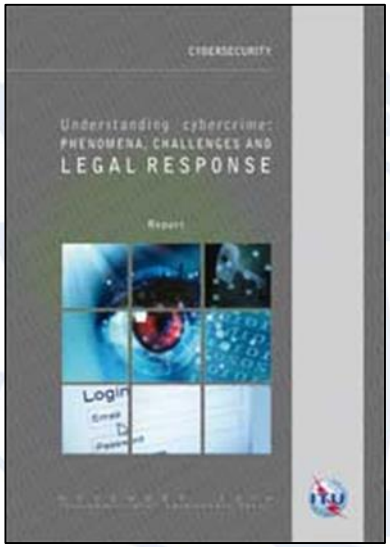
  Barbados, Burundi, Gambia, Lebanon
- Cyber drills conducted all over the world

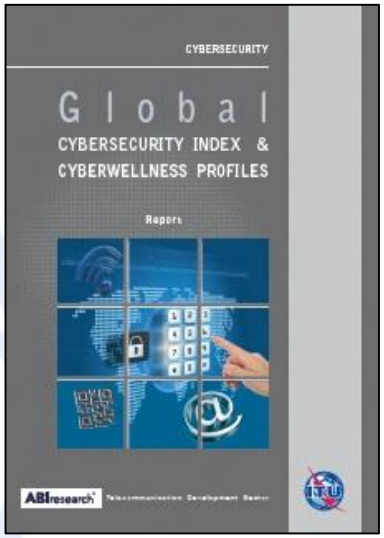
Regional Cyber Drills

- **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)

Publications







Free download from:
http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Publications.aspx

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