As global mobile internet penetration increases the cybercrime and cyberterrorism vector is extended
Global Cybercrime has an estimated cost of US$ 110 Billion per year.
• Every second, **18 adults** become a victim of cybercrime, resulting in more than **1.5 million** cybercrime victims each day on a global level.

• With losses totaling an average of US$197 per victim across the world in direct financial costs, cybercrime costs consumers **more than a week’s worth of nutritious food necessities for a family of four**.

• In the past 12 months, an estimated 556 million adults across the world experienced cybercrime, more than the entire population of the European Union.

• This figure represents **46 % of online adults** who have been victims of cybercrime in the past twelve months, compared with the findings from 2011 (45 percent).

Source: Symantec
More than 1.5 billion web-based cyberattacks took place in 2012
While launching 1.5 billion web attacks throughout 2012

Cybercriminals used 6.5 million unique domains (2.5 million more than in 2011)

Servers seeded with malicious code were detected in the Internet zones of 202 countries around the world.

Source: Kaspersky Lab
U.S. Department of Energy

During an attack on the agency's computers and servers, the personal data of employees and contractors was stolen, but, reportedly, no classified data was leaked.

NY Times, Wall Street Journal and Washington Post
Sensitive information from journalists stolen during 2013

NASA

NASA’s Inspector General reported that 13 APT attacks compromised NASA computers between 2011 and 2012

ITU (December 2012)
Main website compromised during WCIT-12, in the attempt of obstructing a treaty-making conference

India

112 government websites of India had been compromised from December 2011 to February 2012

Japan (September 2012)
Japan faced an onslaught of cyber attacks targeting government websites, universities, banks and hospitals

Almost all governments website of the UN Member States have been attacked between 2011 and 2012 at various levels, from defacement to DDoS, from phishing to data theft

Between 2011 and 2012, some 20 intergovernmental organizations and UN bodies, including IAEA, IMF, UNDP, UN, ITU, have been victims of cyberattacks of various nature
So many differences, so many challenges, so many frameworks
Budapest Convention - Since 2001, some 37 Countries ratified, out of 193 UN Member States

24/7 Network – some 50 countries, since 2001

EU built a cybercrime center, within the EUROPOL structure – Delivery date: 2014

INTERPOL will build a Cybercrime Complex - Delivery date: 2014

Shanghai Cooperation Organization

Commonwealth Cybercrime Initiative, 54 States

EU-US cooperation

EU Directives

African Convention on Cybersecurity, 52 States

FIRST, OIC CERT, GCC CERT, APC CERT and other incident response organizations

Arab Convention on Combating Information Technology Offences
Zero Day Vulnerability and Action

- A zero day vulnerability refers to an unknown malfunction in IT system;

- Zero day attacks include malware, spyware, unwanted access to information.

- This security hole is then exploited by hackers before the vendor is aware - this kind of attack is known as a zero day attack.

- Zero day vulnerabilities are increasingly exploited by cyber criminals and terrorists that use mobile technology.
43 Million $ - 5 bank accounts - 20 Countries – 2,904 ATMs – 2 Attacks – 36 hours – 1 Mobile Internet
Key Challenges

• Lack of adequate and interoperable national or regional legal frameworks

• Lack of secure software and ICT-based applications

• Lack of appropriate national and global organizational structures to deal with cyber incidents

• Lack of information security professionals and skills within governments; lack of basic awareness among users

• Lack of international cooperation between industry experts, law enforcements, regulators, academia & international organizations, etc. to address a global challenge

*Cybersecurity not seen yet as a cross-sector, multi-dimensional concern. Still seen as a technical/technology problem.*
Benefits of more harmonization and streamlining

• Increased efficiency and effectiveness in the detection and analysis of cyber threats

• Greater awareness of risks and adoption of protective behavioral patterns by general public and private sector

• Efficient and effective long-term whole-of-government response to cyberthreats and cybercrime, including national coordinating mechanisms, data collection systems, and effective legal framework

• Strengthened communication between government agencies in cybersecurity matters, between the concerned national stakeholders, including but not limited to ICT policy makers and regulators, judiciary systems, law enforcement, private sector organizations, as well as on international cooperation
ITU – the UN Agency for ICTs and its work

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

2007
ITU Cybersecurity Agenda (GCA) was elaborated and endorsed by ITU Member States
GCA is a framework for international cooperation in cybersecurity

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