Commonwealth Cybersecurity Forum

Yaounde, Cameroon; 25-26 April 2013

Towards a global approach on cybersecurity

Mario Maniewicz

Chief, Infrastructure, Enabling Environment & E-applications

Telecommunication Development Bureau

International Telecommunication Union


Consumer Cybercrime
has an estimated cost
of US$ 110 Billion per year

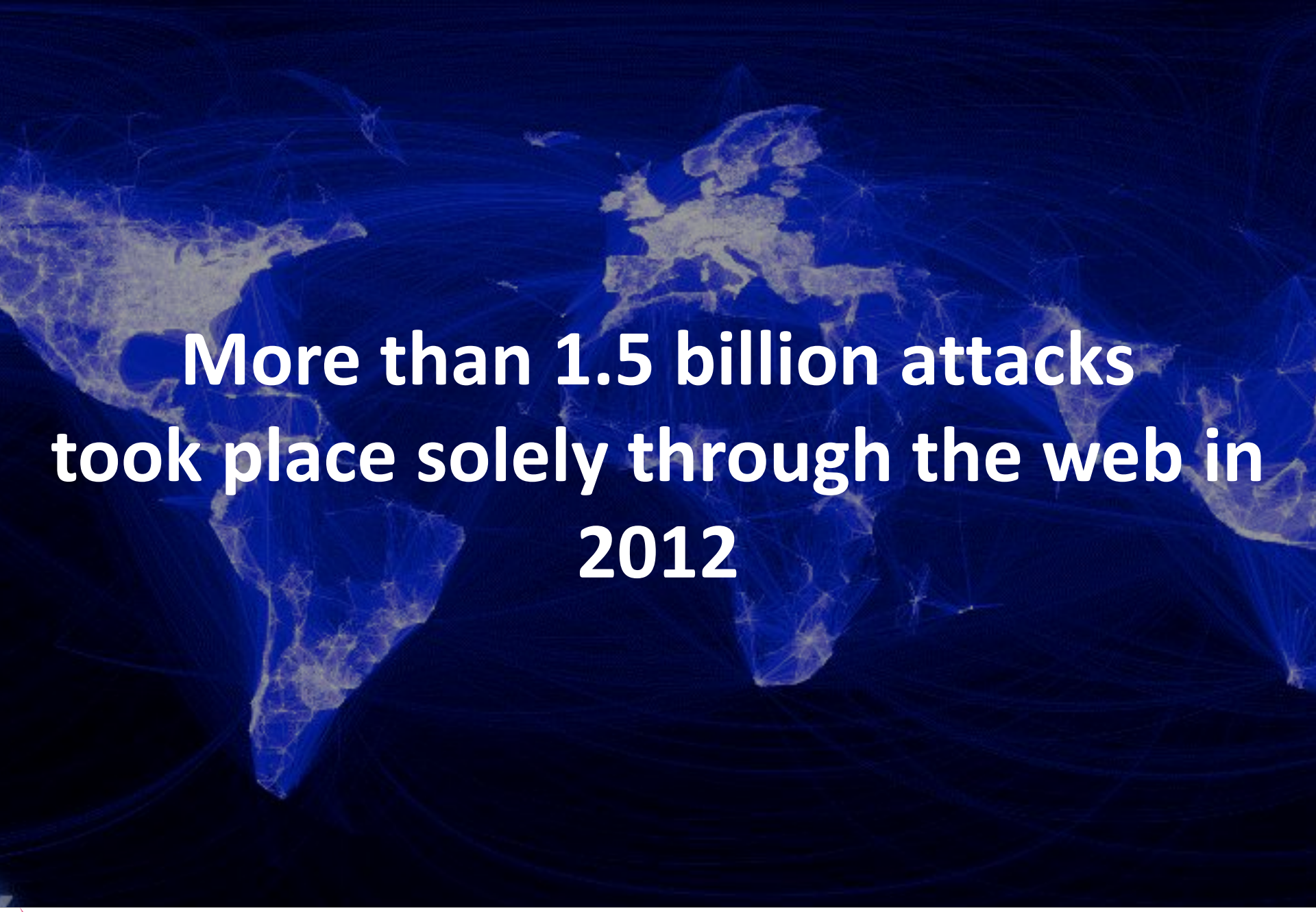
- Every second, **18 adults** become a victim of cybercrime, resulting in more than **1.5 million** cybercrime victims each day on a global level.

- 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 attacks
took place solely through the web in
2012

While launching 1.5 billion web attacks throughout 2012

Cybercriminals used 6.5 million of 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


Everyone is already affected

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.

Twitter

250k were requested to reset their passwords

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


This global trend is expected
to increase
over the upcoming years

Trends for the near future

- Continued rise of targeted attacks and advanced persistent threat
- Attacks targeting cloud-based infrastructures will increase
- Mobile platforms continue to be the emerging market for cybercrime
- Member States are starting to move from defensive to offensive
  Rise of cyber warfare
- United Nations System as one of the main targets identified for 2013
  UN organizations and UN conferences will be affected


So many differences, so many challenges, so many frameworks

WE HAVE PROBLEMS

Cross Border Crime

Lack of Knowledge

Lack of Resources

No Direction

No legal framework

Management Challenges

New Problems

Capital intensive solutions

Need proactive solutions

No emergency telephone numbers

Organisations working in silos

Delays in Response

Lack of international collaboration

Crimes have become organised

Need better early warning system

Addressing different type of attacks

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.

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

EU-US cooperation

Commonwealth Cybercrime Initiative, 54 States

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


Is the UN positioned
to address this challenge?

A UN common position on cybersecurity and cybercrime

In a landscape where cyberspace is becoming a ground for international diplomacy and politics, and a risk to global stability, the UN System must react vigorously:

- To protect itself from the risks posed by cyber threats;
- To help Member States and the international community in facilitating the dialogue aimed at better defend countries against cyber threats and cybercrime, thus contributing to international security and stability

Toward a global framework

- Agreement at the international level on international norms and principles able to regulate cyberspace and acceptable state behavior and codes of conduct within cyberspace

- The establishment of a global platform, where all relevant stakeholders coordinate, cooperate and proactively intervene to resolve cyber incidents and prevent possible escalations

while (in parallel)

- Equip countries with capabilities and know-how
  - Cybercrime legislation
  - Organizational Structures (e.g. CIRTs)
  - Education and training

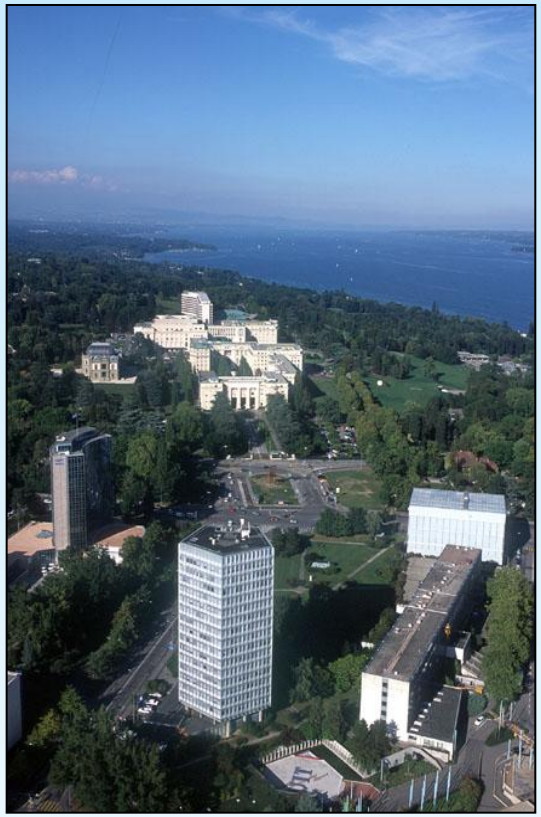
- Work at the regional level
  - Pan-regional agreements

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

What is ITU

- Leading UN specialized agency for information and communication technologies (ICTs).
- Founded in 1865, ITU is the oldest specialized agency in the UN system.
- Global focal point for governments and the private sector with 192 Member States, 532 Sector Members, 148 Associates, and 5 Academia.
- ITU Headquarters in Geneva, Switzerland; 11 regional/area offices; 700 staff of 80 nationalities.

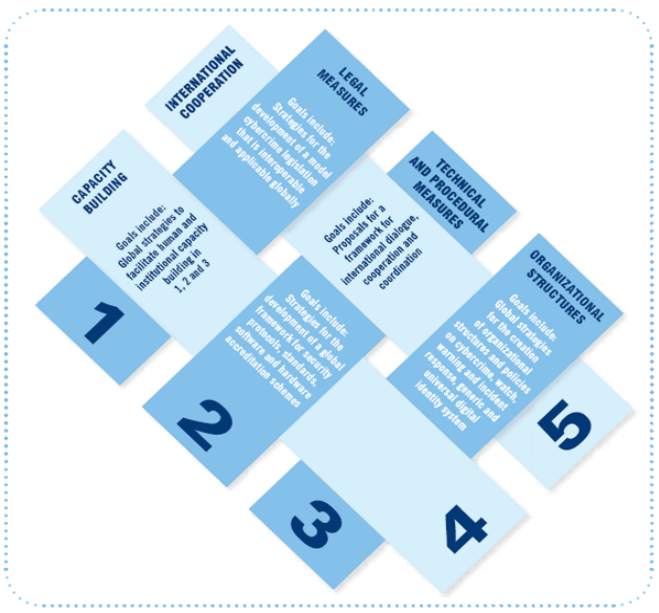


How it is helping the international community

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
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.


Thank you for your attention!
mario.maniewicz [at] itu.int