

Cybersecurity: Taking Stock and Looking Ahead

30 April 2014

Tomas Lamanaskas

Head, Corporate Strategy Division
International Telecommunication Union

Context

Different Perspectives of Cybersecurity



or



It is first of all about trust and confidence necessary to derive benefits from ICTs

Global losses due
to cybercrime $\approx$
500 billion USD
annually





Building confidence and security in the use of ICTs

G

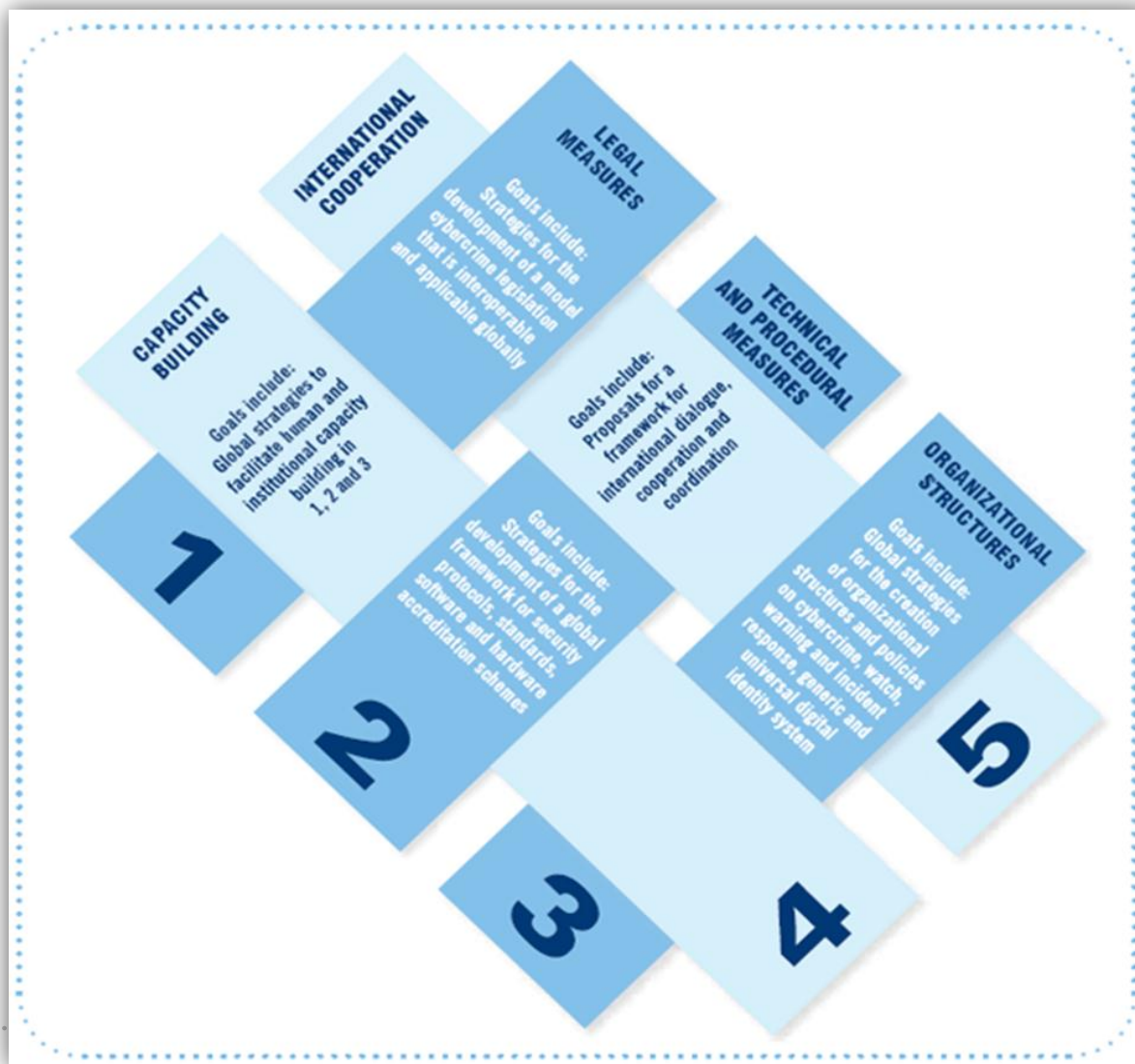
C

A

GLOBAL
CYBERSECURITY
AGENDA



International
Telecommunication
Union



Cybersecurity Challenges

THE SCALE OF CONSUMER CYBERCRIME

378 MILLION VICTIMS PER YEAR



NEARLY 2.8 TIMES AS MANY BABIES BORN EACH YEAR



1 MILLION +
VICTIMS PER DAY

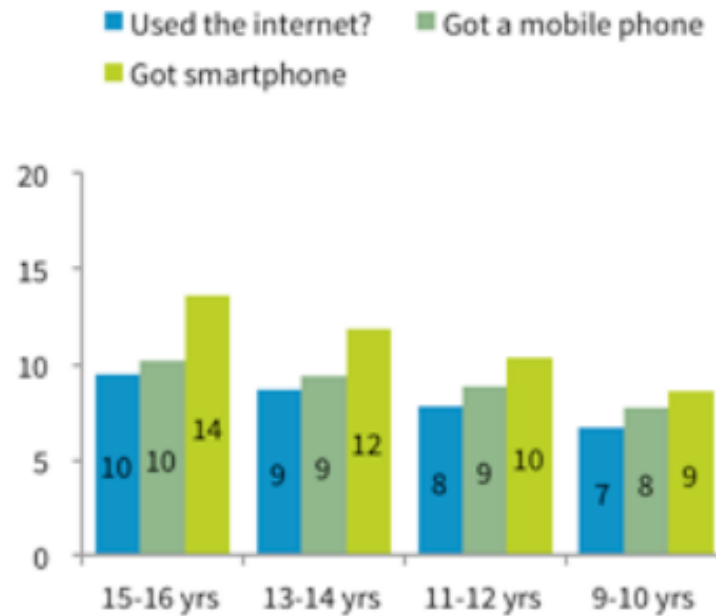
ENOUGH TO FILL WEMBLEY STADIUM (ENGLAND) MORE THAN 10 TIMES



12 VICTIMS PER SECOND

Need for Child Online Protection

Fig. 4: Age of first internet use, first mobile phone and first smartphone by age



Q5 How old were you when you first used the internet?

Q6 How old were you when you got your first mobile phone (a phone which is not a smartphone)?

Q7 How old were you when you got your first smartphone?

Base: All children who use the internet

FUNDED BY:



Safer Internet Programme
European Commission
(SI-2012-KEP-411201)



Digital Identities

Total
Breaches



253

2013

+62%

156

2012

Total Identities
Exposed



552 Million

2013

+493%

93 Million

2012

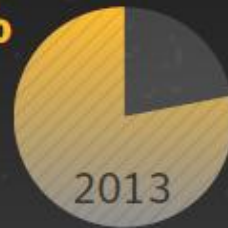
Scanned Websites With Vulnerabilities ...



53%



77%



+25%
pts

... % of Which Were Critical

24%



16%

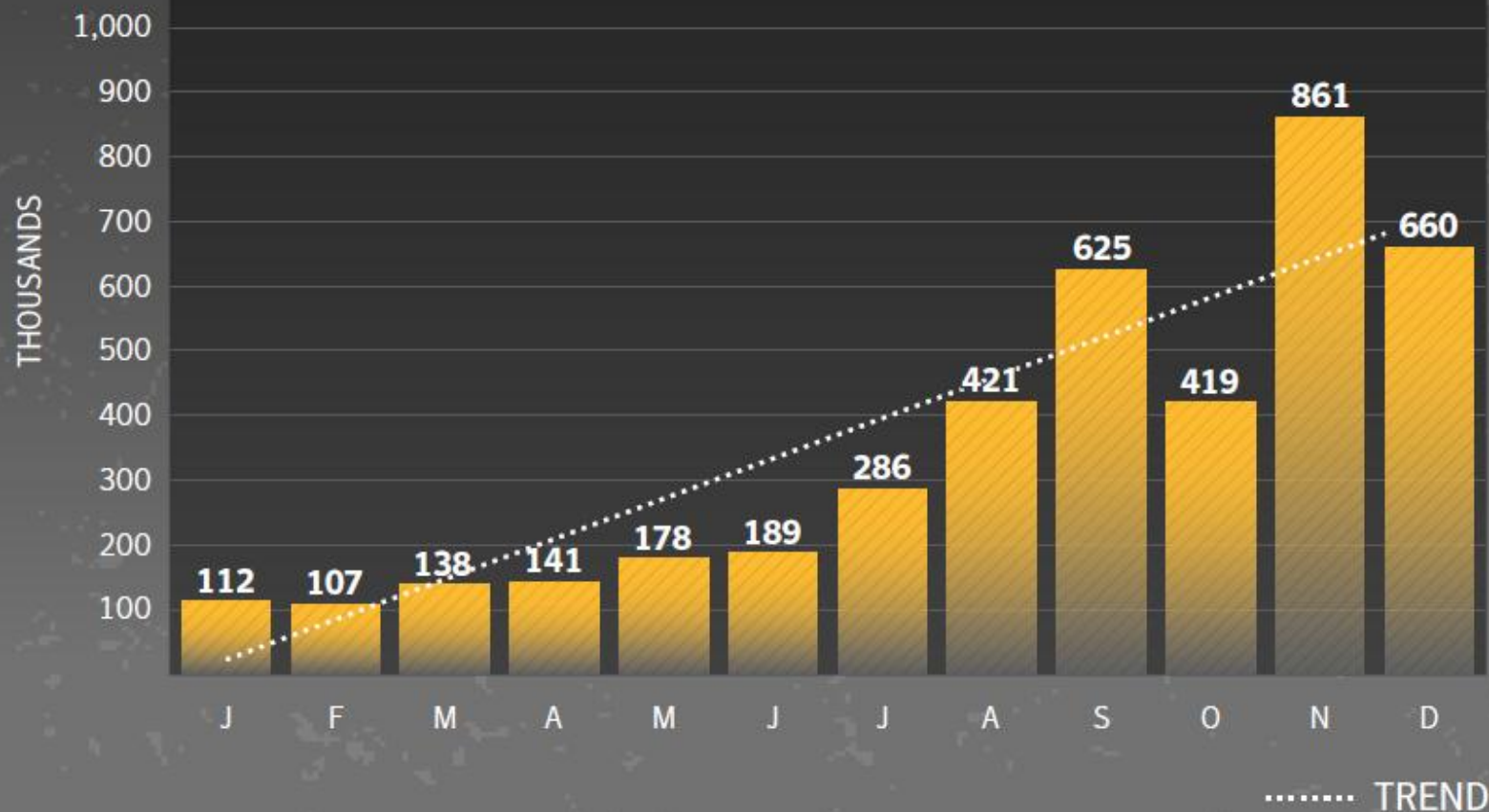


-8%
pts

1 IN 8 sites
had critical
unpatched
vulnerabilities

Ransomware Over Time, 2013

Source: Symantec

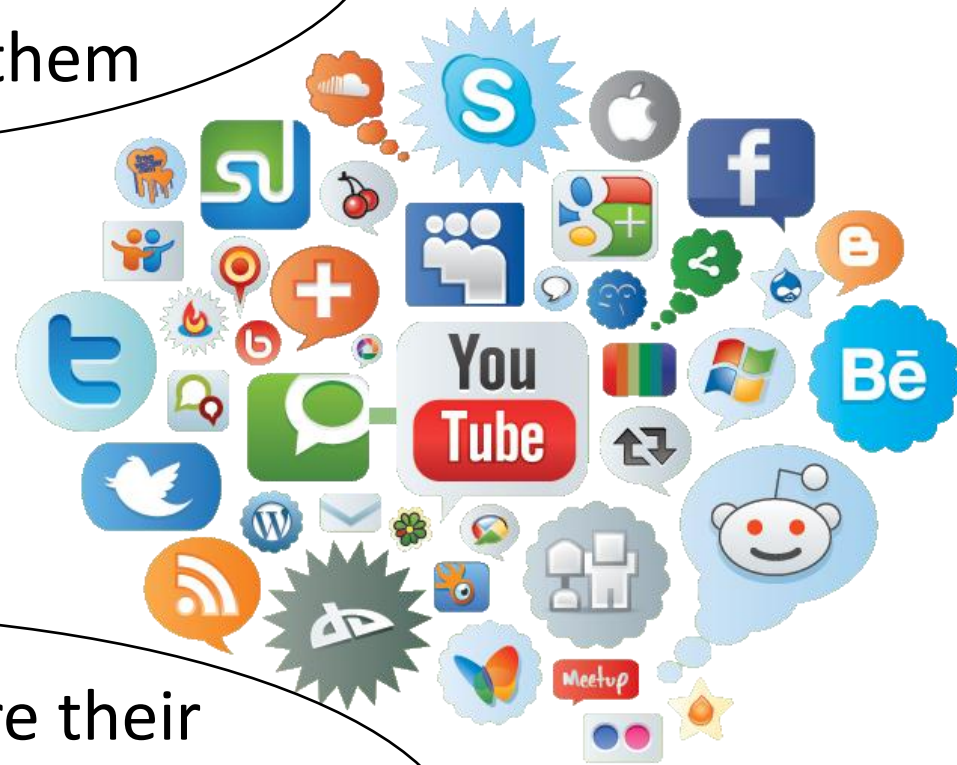


38% mobile users
experienced mobile
cybercrime

Only 50% take even
basic security
precautions



12% social media users say
someone has hacked into
their social network account
and pretended to be them



25% continue to share their
social media passwords with
others and a third connect
with people they don't know

Industries at Greatest Risk of Being Targeted by Spear Phishing



Mining

1 IN **2.7**



Public Administration (Gov.)

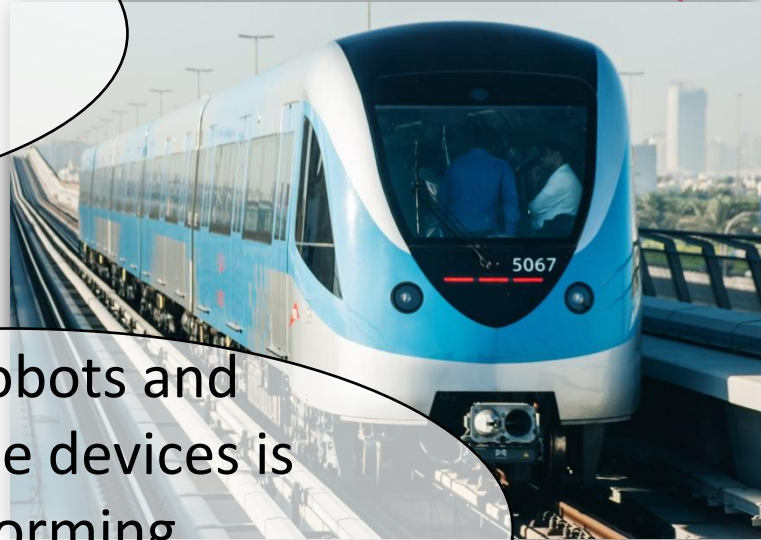
1 IN **3.1**



Manufacturing

1 IN **3.2**

Critical infrastructure is increasingly ICT dependent



Use of robots and implantable devices is transforming cyberthreats to physical threats

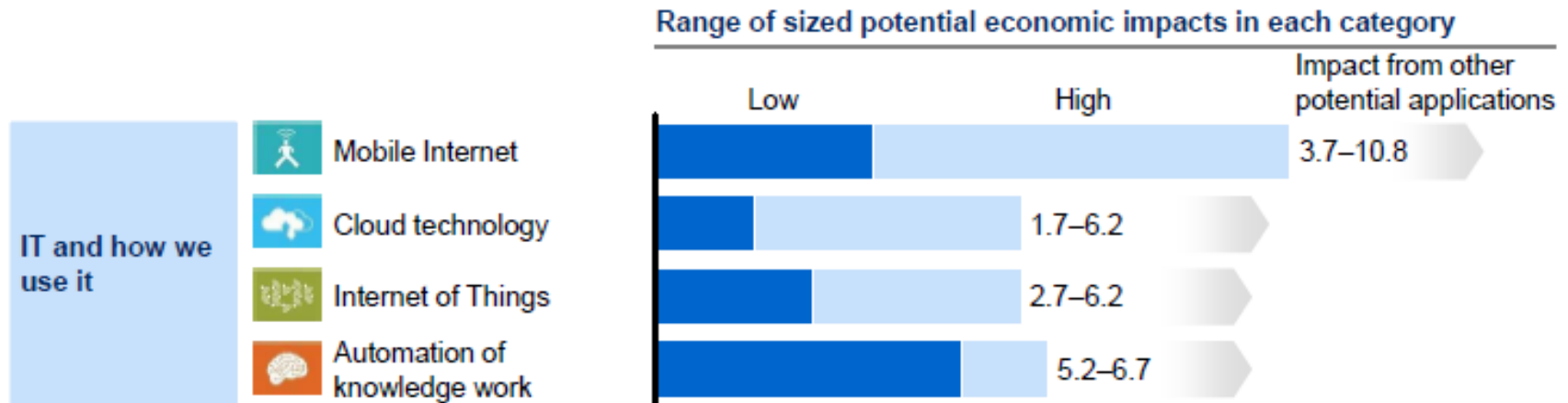


Number of **networked devices** will potentially reach 50 billion connected objects by 2020



By 2025, these technologies could have economic impact in the trillions

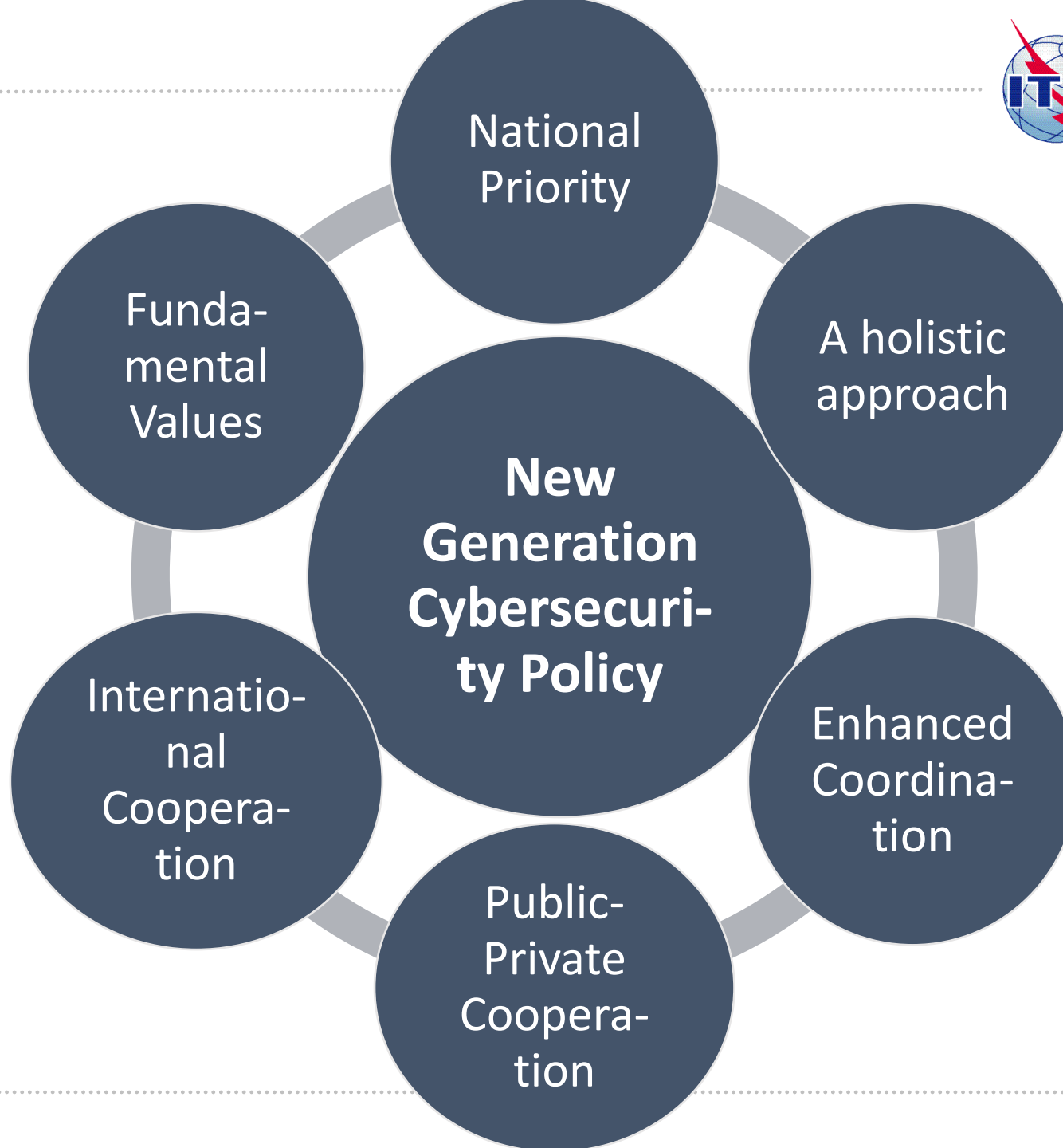
\$ trillion, annual by 2025

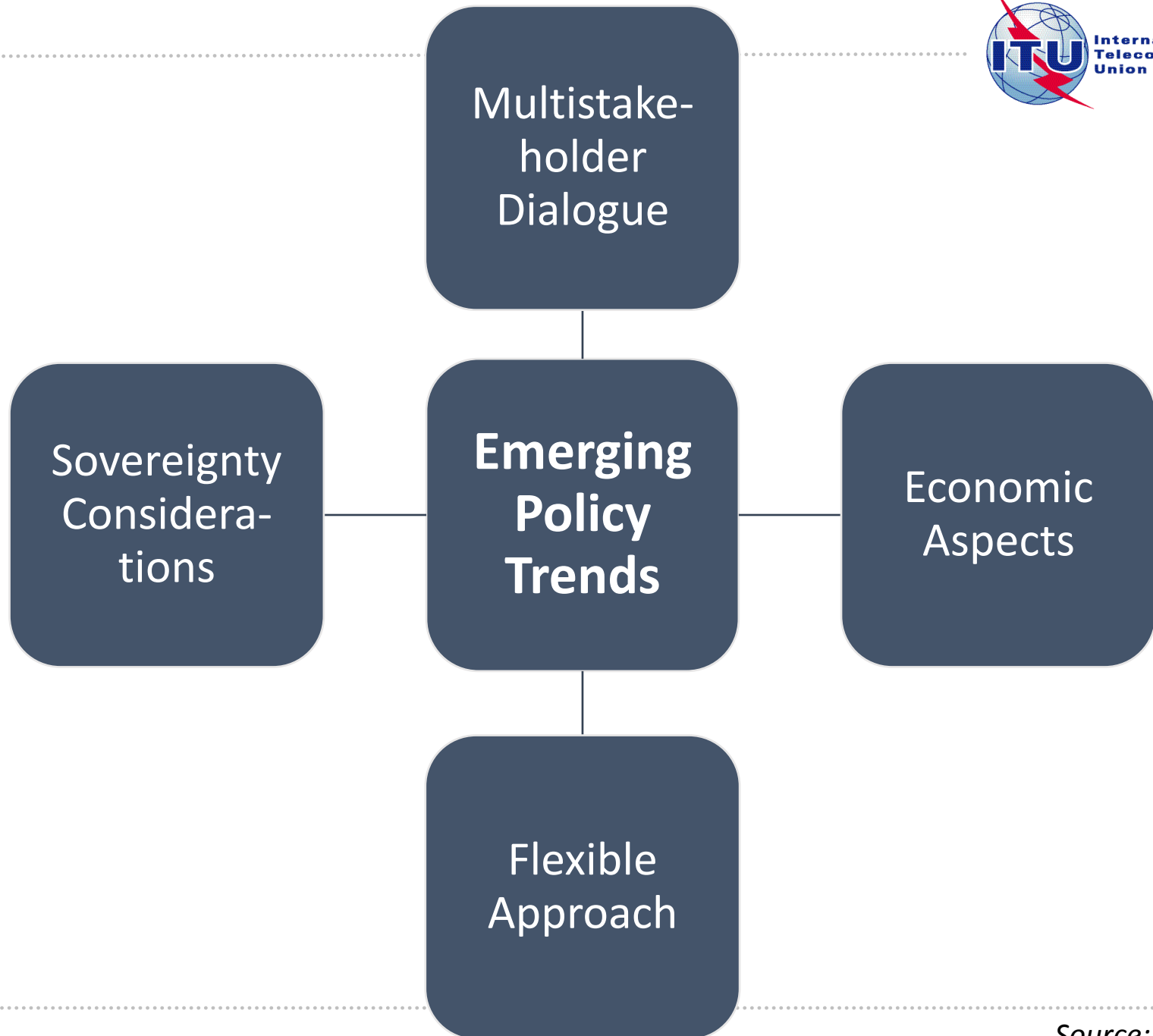


Source: McKinsey Global Institute

...but new risks emerge, and realization of potential of new technologies needs trust and confidence

Addressing the Challenges





International Cooperation – Regional and Plurilateral

Budapest Convention (2001), 41
Countries ratified/acceded



G8 24/7 Network – some 50
countries, since 2001

Set of confidence-building
measures (CBMs) to reduce
the risks of conflict
stemming from the use of
ICTs



UN Efforts

- Resolution 68/243 of the UN General Assembly on “Developments in the field of information and telecommunications in the context of international security” (2013)
- Resolution 68/167 of the UN General Assembly on “The Right to Privacy in the Digital Age” (2013)
- Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2013)
- Resolution 20/8 of the Human Rights Council on “The promotion, protection and enjoyment of human rights on the Internet” (2012)
- Resolution 57/239 of the UN General Assembly on “Creation of a global culture of cybersecurity” (2002)



World Conference on International Telecommunications (WCIT-12)

WCIT-12 set the ground for international cooperation on certain cybersecurity-related matters

- Article 6, ITRs: **Security and robustness of networks**
- Article 7, ITRs: **Unsolicited bulk electronic communications**





EUROPEAN
COMMISSION



New EU Initiatives

Proposal for a **Directive** of the European Parliament and of the Council **concerning measures to ensure a high common level of network and information security across the Union** (COM (2013) 48 final)

Proposal for a **Regulation** on **Electronic identification and trust services for electronic transactions in the internal market** (COM(2012) 238 final)

Joint Communication of the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: **Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace** (JOINT (2013) 1)

Standardization



Economic Impact
of Standardization

**Adds 0.3% - 1% to
the GDP**

Source: European Commission

ITU-T Study Group 17 – Security

- **Over 70 standards** (ITU-T Recommendations) focusing on security
- Key areas of current work:
 - Cybersecurity
 - Child Online Protection
 - Security architectures and frameworks
 - Countering spam
 - Identity management
 - Security of applications and services for the Internet of Things, web services, social networks, cloud computing and Big Data

Increasing Awareness

Low Hanging Fruit Still Exists

“80% or more of currently successful attacks exploit weakness that can be avoided by following simple best practice, such as updating anti-malware software regularly”

The UK Cyber Security Strategy, 2011



Increasing Awareness

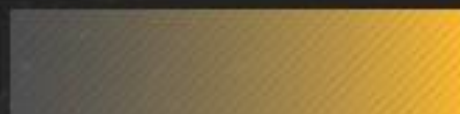
Top Causes of Data Breach, 2013

Source: Symantec

Number
of Incidents



Hackers



34%

87

Accidentally
Made Public



29%

72

Theft or Loss
of Computer
or Drive



27%

69

Insider Theft



6%

15

Unknown



2%

6

Fraud



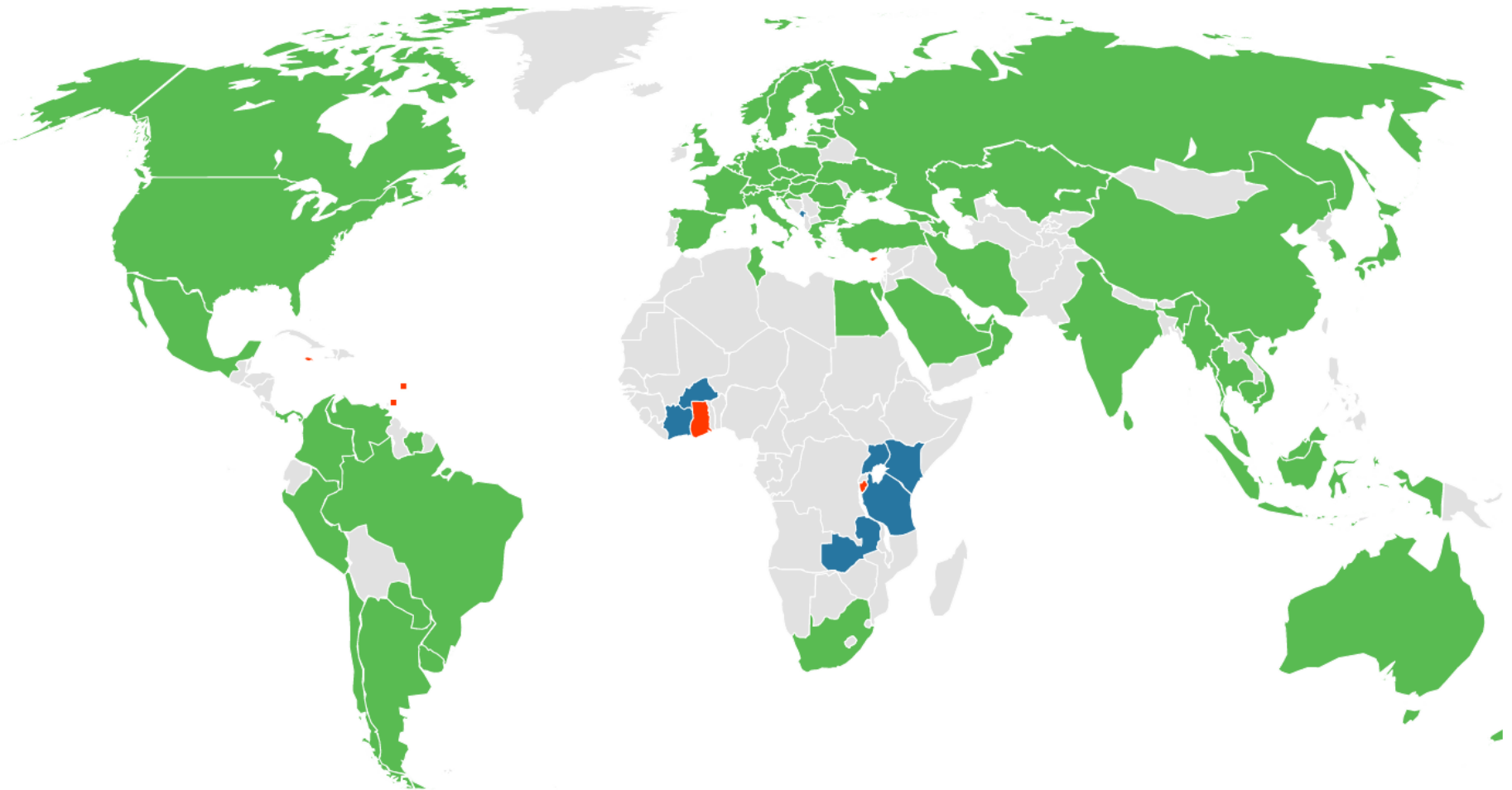
2%

4

TOTAL

253

Institutional Structures: CIRTs



 Established with the assistance of ITU

 In progress with the assistance of ITU

Some Further Relevant ITU Work

ABIresearch[®]



Global Cybersecurity Index



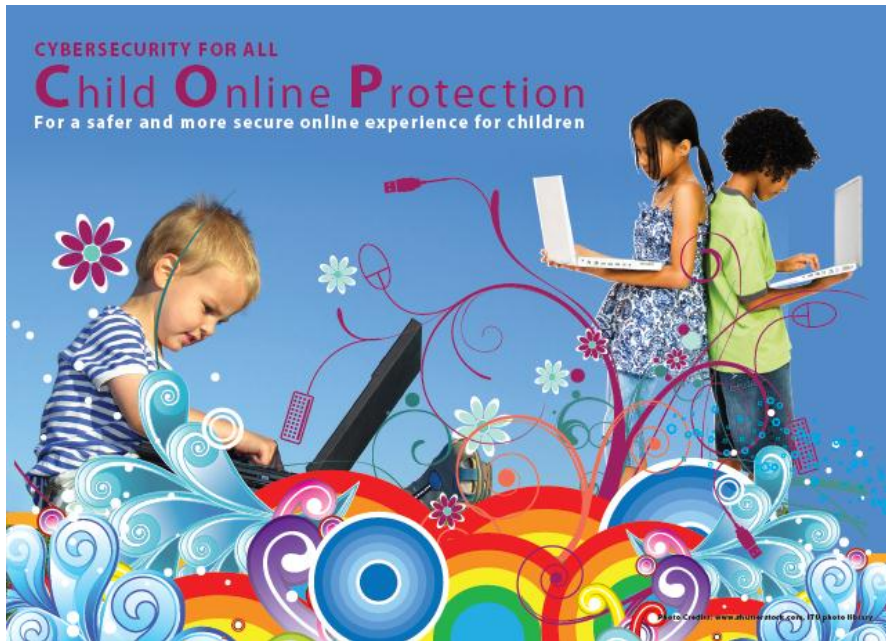
Key Services:

- real-time analysis, aggregation and dissemination of global cyber-threat information
- an early warning system and emergency response to global cyber-threats
- training and skills development on the technical, legal and policy aspects of cybersecurity

Joined by 149 Countries

IMPACT

Child Online Protection Initiative

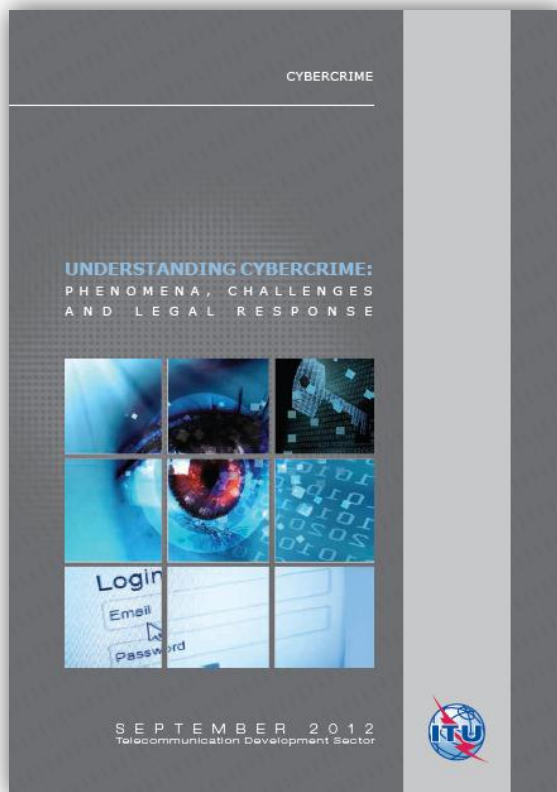


Key Objectives:

- Identify risks and vulnerabilities to children in cyberspace
- Create awareness
- Develop practical tools to help minimize risk
- Share knowledge and experience

Partners:

- 10 international organizations
- 33 civil society organizations
- 13 private sector organizations

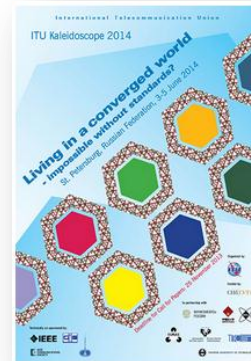


Upcoming ITU Events



➔ **Cyber Drill, 15-16 May 2014, Istanbul, Turkey**

ITU Kaleidoscope, 3-5 June 2014, Saint Petersburg, Russian Federation ←



➔ **WSIS+10 High Level Event, 10-13 June 2014, Geneva, Switzerland**

Global Symposium for Regulators, 3-5 June 2014, Manama, Bahrain ←



➔ **ITU Plenipotentiary Conference, 20 Oct – 7 Nov 2014, Busan, Republic of Korea**



ITU Telecom World, 7-10 December 2014, Doha, Qatar ←



Thank You