ICT and Security

The Need to Move from "Consumers" to "Developed" Countries

Dr. Imad Y. Hoballah
Acting Chairman and CEO,
Head of Telecommunications Technologies Unit,
Telecommunications Regulatory Authority (TRA), Lebanon

WSIS Approach

WSIS serves as a global reference for:

Improving Connectivity

Universal, Ubiquitous, Equitable, Non-Discriminatory and Affordable Access to, and Use of, ICTs

WSIS Plan of Action includes:

C1. The role of public governance authorities and all stakeholders in the promotion of ICTs

C2. Information and communication infrastructure

C3. Access to information and knowledge

C4. Capacity building

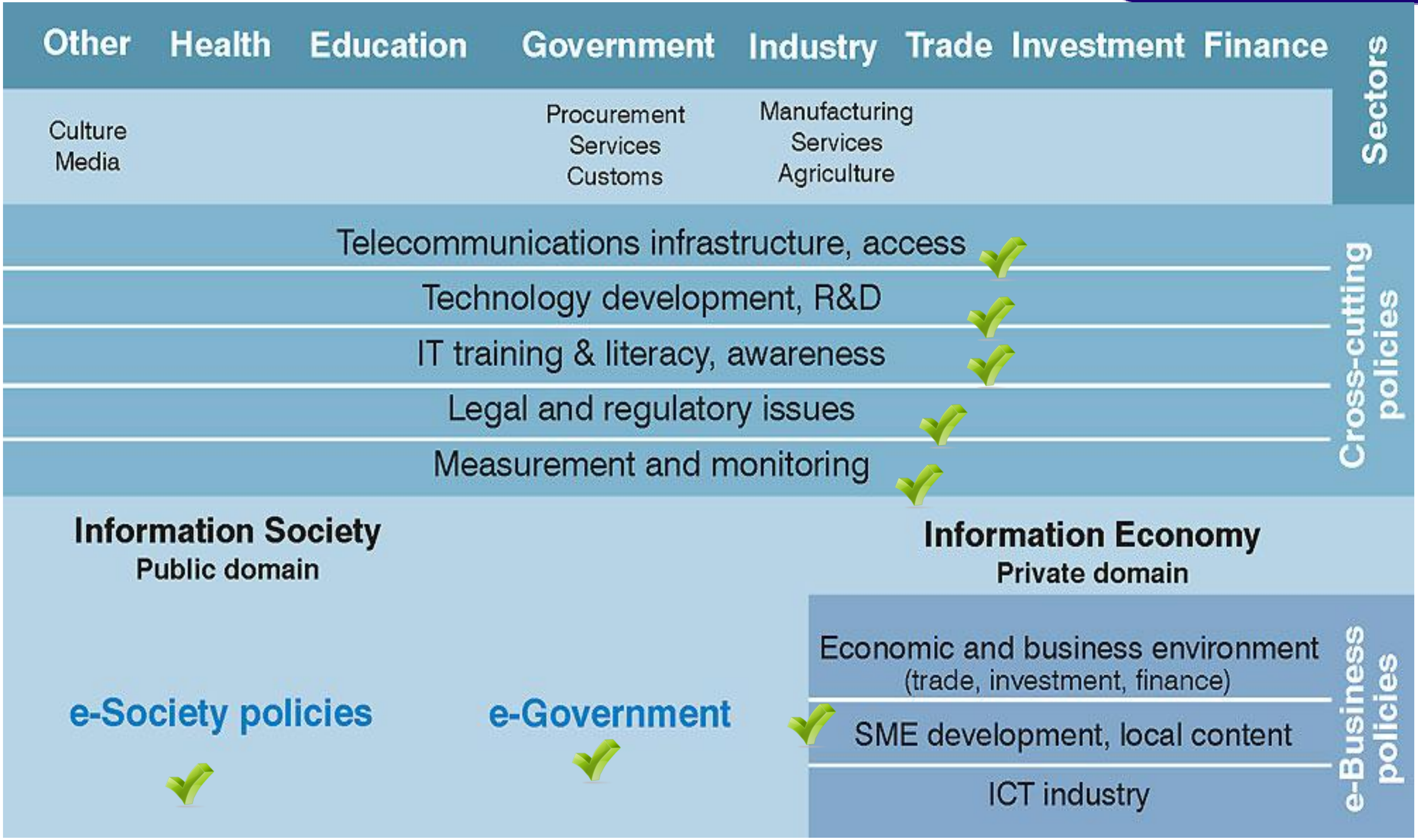
C5. Building confidence and security in the use of ICTs

C6. Enabling environment

C7. ICT Applications:

E-government,
E-business,
E-learning,
E-health,
E-employment,
E-environment,
E-agriculture,
E-science

ICT Policy Framework



Other Health Education Government Industry Trade Investment Finance

Sectors

Culture
Media

Procurement
Services
Customs

Manufacturing
Services
Agriculture

Cross-cutting policies

Telecommunications infrastructure, access ✓

Technology development, R&D ✓

IT training & literacy, awareness ✓

Legal and regulatory issues ✓

Measurement and monitoring ✓

Information Society
Public domain

Information Economy
Private domain

e-Society policies ✓

e-Government ✓

e-Business policies

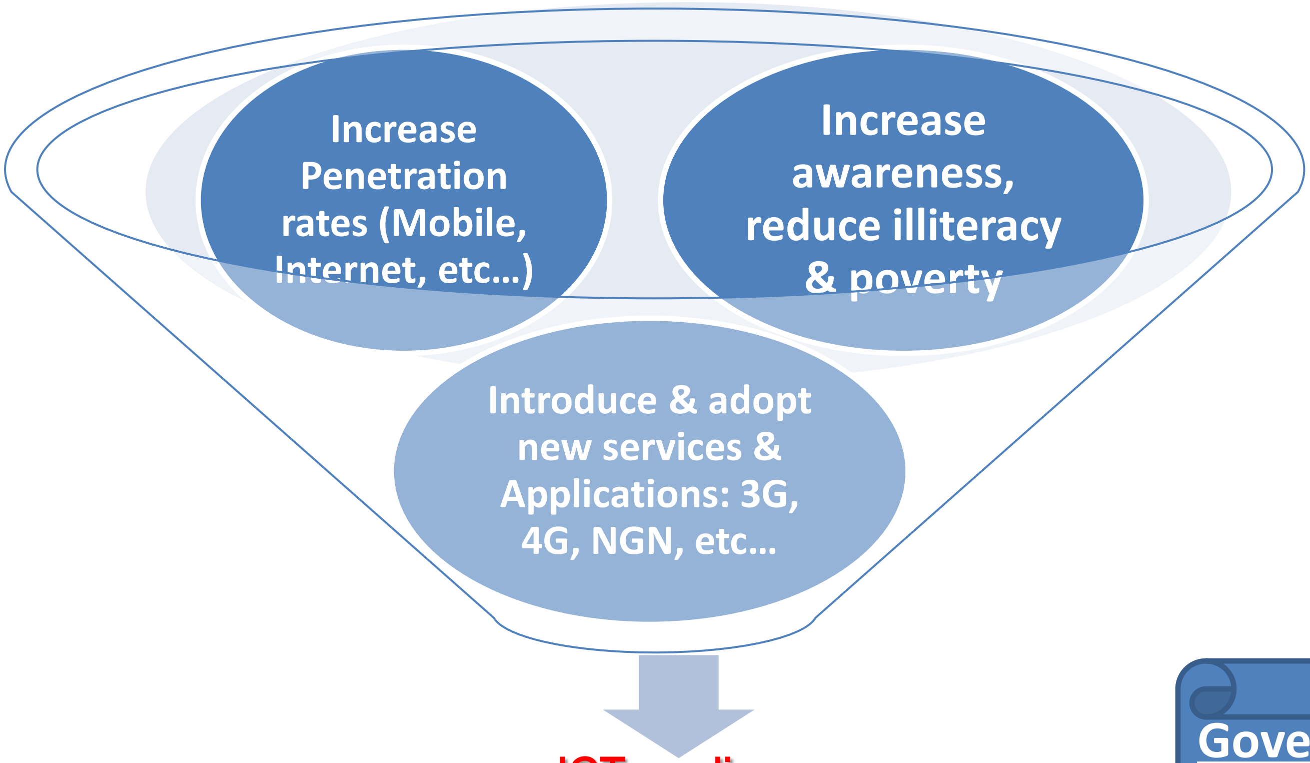
✓ Economic and business environment
(trade, investment, finance)

SME development, local content

ICT industry

Source: United Nations Conference on Trade and Development

Reports Show that Many Developing Countries Have Succeeded in Improving Their ICT Indicators



Increase Penetration rates (Mobile, Internet, etc…)

Increase awareness, reduce illiteracy & poverty

Introduce & adopt new services & Applications: 3G, 4G, NGN, etc…

ICT readiness

ICT affordability

ICT usage

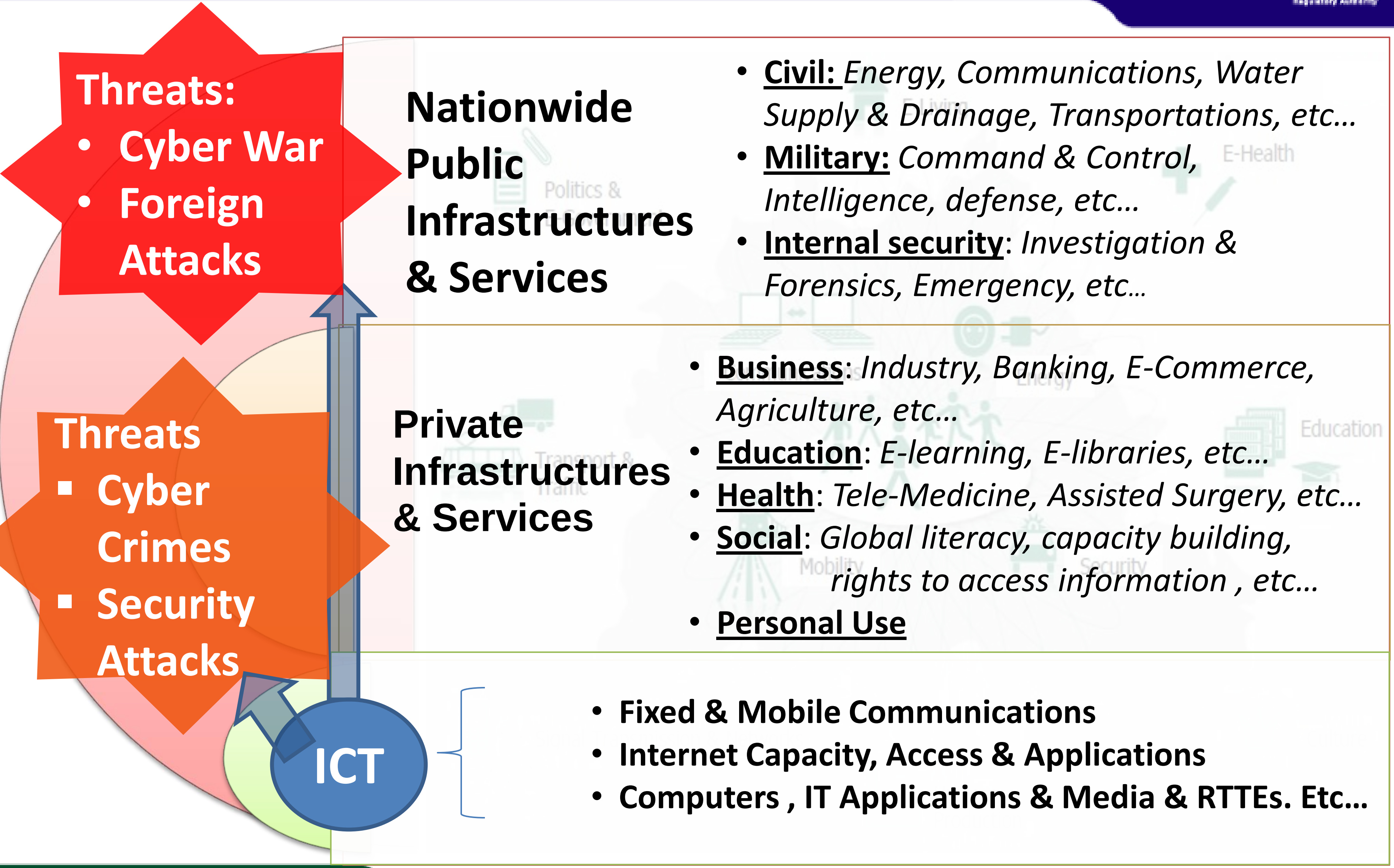
ICT impact

Governments and businesses have succeeded in creating high ICT consumption communities…

Results Show that Major Developing Countries Have Succeeded in Improving Their ICT Indicators

And?

Resulting in Increase of ICT involvement



Threats:

- **Cyber War**
- **Foreign Attacks**

Threats

- **Cyber Crimes**
- **Security Attacks**

Nationwide Public Infrastructures & Services

- **Civil:** *Energy, Communications, Water Supply & Drainage, Transportations, etc…*
- **Military:** *Command & Control, Intelligence, defense, etc…*
- **Internal security**: *Investigation & Forensics, Emergency, etc…*

Private Infrastructures & Services

- **Business**: *Industry, Banking, E-Commerce, Agriculture, etc…*
- **Education**: *E-learning, E-libraries, etc…*
- **Health**: *Tele-Medicine, Assisted Surgery, etc…*
- **Social**: *Global literacy, capacity building, rights to access information , etc…*
- **Personal Use**

ICT

- **Fixed & Mobile Communications**
- **Internet Capacity, Access & Applications**
- **Computers , IT Applications & Media & RTTEs. Etc…**

Governmental Involvement in Cyber Security, Attacks, and Wars

- According to reports: **Cyber attacks on governments and companies have increased by more than 500 % over the last two years**
- **April 2009: The UK GOV confirms plans for a £2B tracking system** to snoop network traffic for any criminal or dangerous activity, known as the **Interception Modernization Program (IMP)**
- **June 2009: The US announces the formation of the US Cyber Command**, an official military body dedicated to:
  - Defense against cyber-invasion
  - Attacks against enemy computer networks
- **November 2009: India announces similar plans to the UK's IMP,** partly in response to reports that terrorists involved in massive attacks in Mumbai used VoIP and Google Earth
- **Recent Years**, **Unit 8200 within the Israeli intelligence,** dedicated for Cyber war and attacks, was revealed (more information)
- **Feb 2011**: **Cyber attacks on major stock exchanges**

Cyber Crime and Security Attacks
The March 2011 French Case

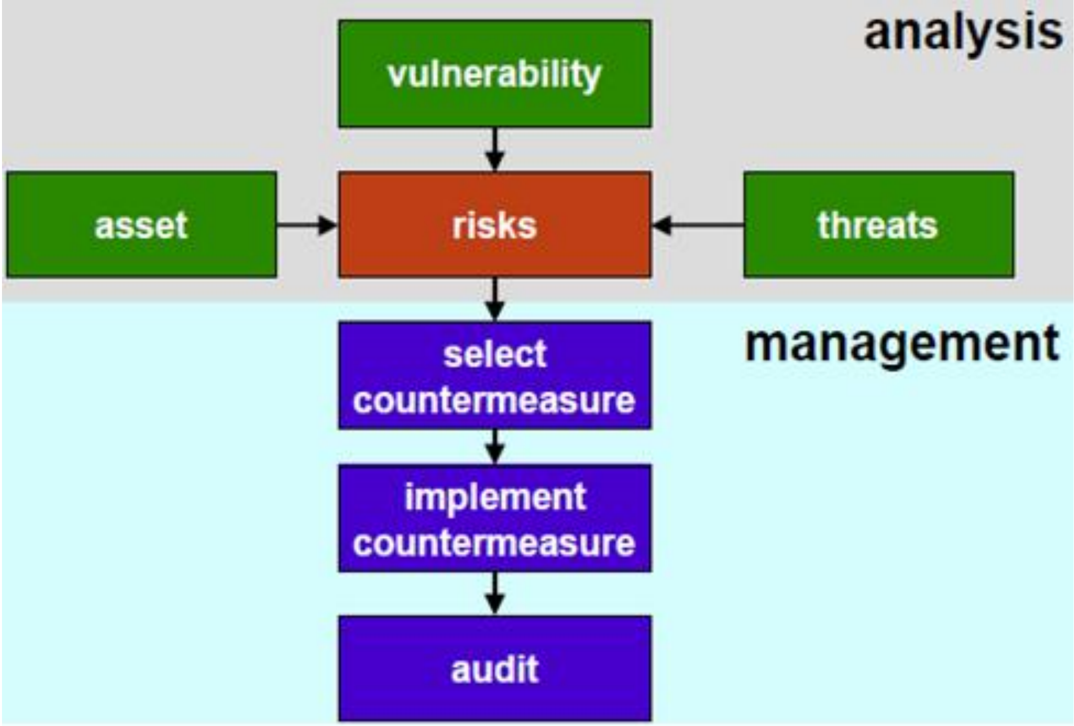
Target: French GOV (documents on international economic affairs)

- François Baroin, French Budget Minister:
  - **“Attacks came from addresses located outside of France”**
- A senior French official:
  - **“We know that certain information was redirected to Chinese sites, but we can't tell much more than that"**
- Patrick Pailloux, DG of the French National Agency for IT Security:
  - ***“The actors were determined professionals and organized.***
  - ***It is the first attack of this size & scale against the French State"***
- Reports:
  - **“Hackers used a Trojan to infiltrate systems having used spear phishing messages that were sent to French government workers”**

Cyber Crime and Security Attacks
The February 2011 UK Case

- A report commissioned by the Cabinet Office into the integrity of computer systems and threats of industrial espionage:
  - **“Cyber Crime costs the UK more than £27B a year”**
  - UK loses £9.2B a year through the theft of innovations and designs (IPR)
  - Industrial espionage, including firms spying on each other, costs £7.6B
  - Cyber crime costs citizens £3.1B and the government £2.2B a year
- Last year's Strategic Defense and Security Review (SDSR):
  - **“Attacks on the UK's IT systems were identified as one of the four (4) most serious threats to national security, alongside terrorism, natural disasters and major accidents**
- Baroness Neville-Jones, UK Security Minister:
  - ***“Some of the cyber crime activity was "state-sponsored" but although the government had the ability to strike back it was "anxious not to get into a barney with “friendly countries over the issue”***

But Analysis of Regional ICT Security Sector Management Shows that Security Emerges Out of Individual Business Decisions



- Local Industry / expertise?
- Purchasing solutions: principles and procedures

ICT Security Solutions as a Corporate or Individual Business Decisions

1. Background of vendors, brokers, experts?
2. Solutions in terms of technological "boxes and fixes"?
3. Hidden backdoors & vulnerabilities?

Must we re-think the purchase and support decision?

ICT Challenges: Digital Divide

“There is work to be done to reduce the so-called digital divide between the ***technology haves and have-nots****”*

Donald J. Johnston

Former Secretary-General of the OECD

There is a Growing Industry Divide for ICT and ICT Security

- ICT is at the center of Economic Development for all sectors
- ICT is a must to advance and avoid the economic and social divides
- National and regional experts and reliable solutions are not accessible
- People/operators (public & private) are seeking ICT solutions based on
  - entrepreneurship and regular corporate or individual business plans (off-the-shelf products, lowest price, outsourcing, some customization, etc.) – quickest and highest returns!
  - >95 % of ICT products/solutions (and experts) are from foreign sources (push/pull) → unable to control all elements
  - almost blind trust
- It is easy to believe that attempts for ICT security are getting us there!
- What role does (and should) the government play?
- Are there National Economic Policies with Security-centric ICT strategy?
- What does all of the above lead to?

ICT Security — Policy Recommendations (1/2)

- Recognize that ICT is a national security concern, impacting economy, knowledge, and society
- Develop a **National Security-Centered ICT policy and strategy based on:**
  - **National Security Drivers** rather than normal business planning only
  - Must be **Championed and Managed at the Highest Level – Who is responsible?**
- Develop **Awareness** at the Highest Level of National Security Decision-Making
- Increase security **Knowledge**, promote **innovation** & incentivize ICT **industry**
- Dedicate National **R&D** Capacity Programs
  - Incentivize **investments in ICT Security R&D**: Public, Private, Civil , Military, ..
- Empower & Encourage **academic research on cryptography, protocols, devices, products, applications, and security**
- Create a favorable **climate to retain and attract resources and skills**
- Encourage **Public Private Partnership (PPP)** to develop ICT Security solutions and products, and propose and provide solutions to continuously upgrade information security level
- Enhance **Regional (and International) Cooperation** on ICT policy, security, and harmonization
- Issue proper **legislations to combat electronic crimes** and establish a “UNIT(s)” to deal with electronic crimes and manage complaints
- **Separate military, security forces, civil defense networks from civilian networks**

ICT Security — Policy Recommendations (2/2)

- Manage the national need for ICT security and the potential **disadvantages of imported solutions/experts (especially dealing with ICT security of national, critical infrastructures as "individual business transactions")**
  - Attract and develop native capabilities and skills for this purpose
- **Establish and enforce procedures for selecting, approving, auditing & conforming**
  - Suppliers, operators, staff & experts
  - Telecom applications, equipment and devices
  - Safety and security of ICT networks
  - Network planning, management and O&M with security standards
  - Protecting against infringements (domestic & foreign, commercial & military)
- Promote the development of **standards and controls to protect personal and data privacy and confidentiality** of data exchanged among agencies
- Establish and implement **measures to protect consumers & personal data**
- Enhance the contribution within the ITU
- **CHALLENGE: DO ALL OF THE ABOVE WHILE SPEEDING UP ICT DEVELOPMENT AND MAINTAINING INTERNET FREEDOM!**

Thank You

www.tra.gov.lb