Տեղեկութիւններու եւ Հաղորդակցութեանց Արհեստագիտութիւններու անվտանգութիւն Լիբանանի մէջ

Դոկտ. Իմատ Հուպալլահ
Գործող Նախագահ եւ Ընդհանուր Տնօրէն,
Հեռահաղորդակցութեան Արհեստագիտութեանց Բաժանմունքի Ղեկավար
Հեռահաղորդակցութեանց Կանոնակարգիչ Իշխանութիւն, Լիբանան

Հայկազեան համալսարան , 13 Յունուար 2011

Information and Communications Technologies (ICT) Security In Lebanon

Haigazian University, 13 January 2011

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

Agenda

- Definition, Role & Benefits of ICT
- ICT & Broadband Diffusion – Facts & Figures
- ICT Threats - Secondary Effects
- ICT Security - The ITU Framework
- The Lebanese Case

Definition, Role, and Benefits of ICT

Information & Communications Technologies (ICT) Definition

ICT is an *umbrella term*

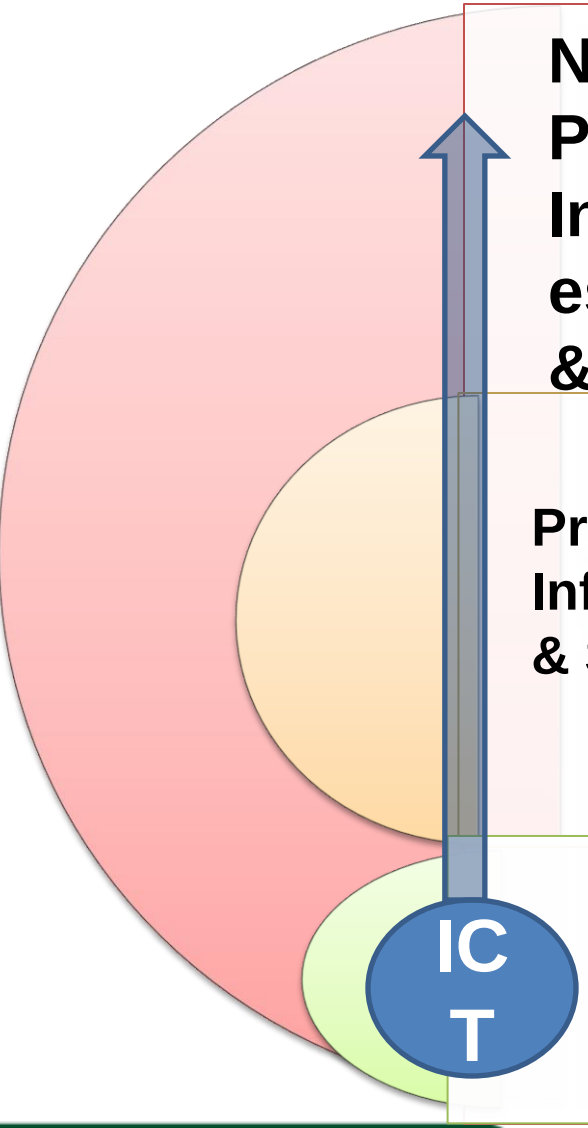
- *Any communication device:*
  - *Radio*
  - *TV*
  - *Fixed & Cellular phone*
  - *Computer*
  - *Network hardware and software*
  - *Satellite systems*

+ *Various services and applications associated with them*

  - *videoconferencing and distance learning*

Note: ICT is often spoken of in a particular context, such as ICT in education, health care, or libraries.

ICT- Role



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**

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

ICT- Benefits

- **Poverty alleviation**
- **Health - The fight against disease**
- **Education - Distant learning**
- **Development - Sustainable development & awareness**
- **HR - Empowerment of marginalized groups**
- **Economy - Productivity & infrastructure development**

ICT Benefits (Cont.)
Impact of IT on the Worldwide Economy

Significant impact of the IT sector on the global economy

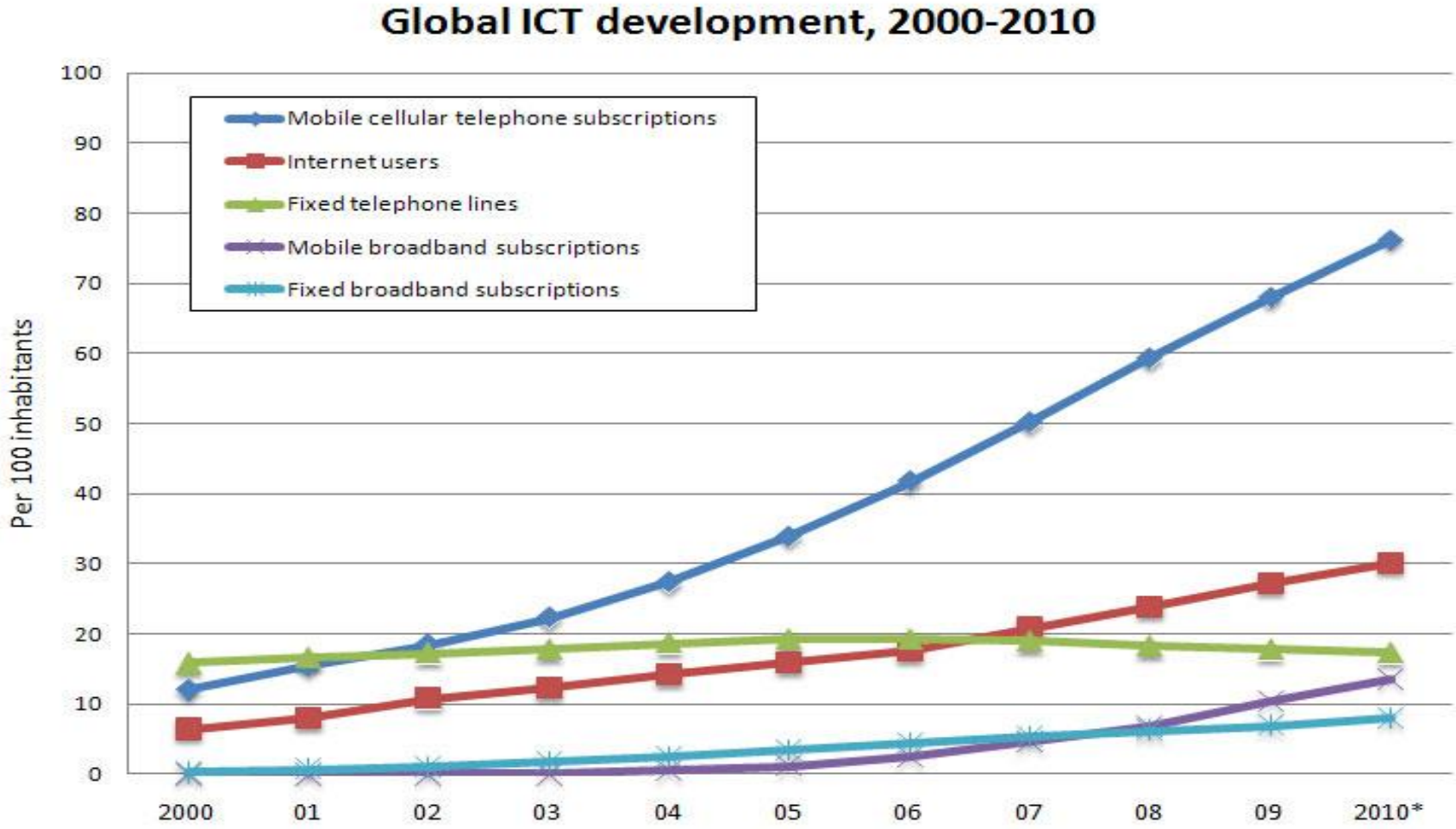
- 1.1 million projects in the IT sector
- 11 million jobs in the information technology sector - high-income jobs
- Annual tax returns, worth about $900B
- An annual contribution of $ 1.7 trillion to the development of the global economy

ICT- Benefits (cont.)

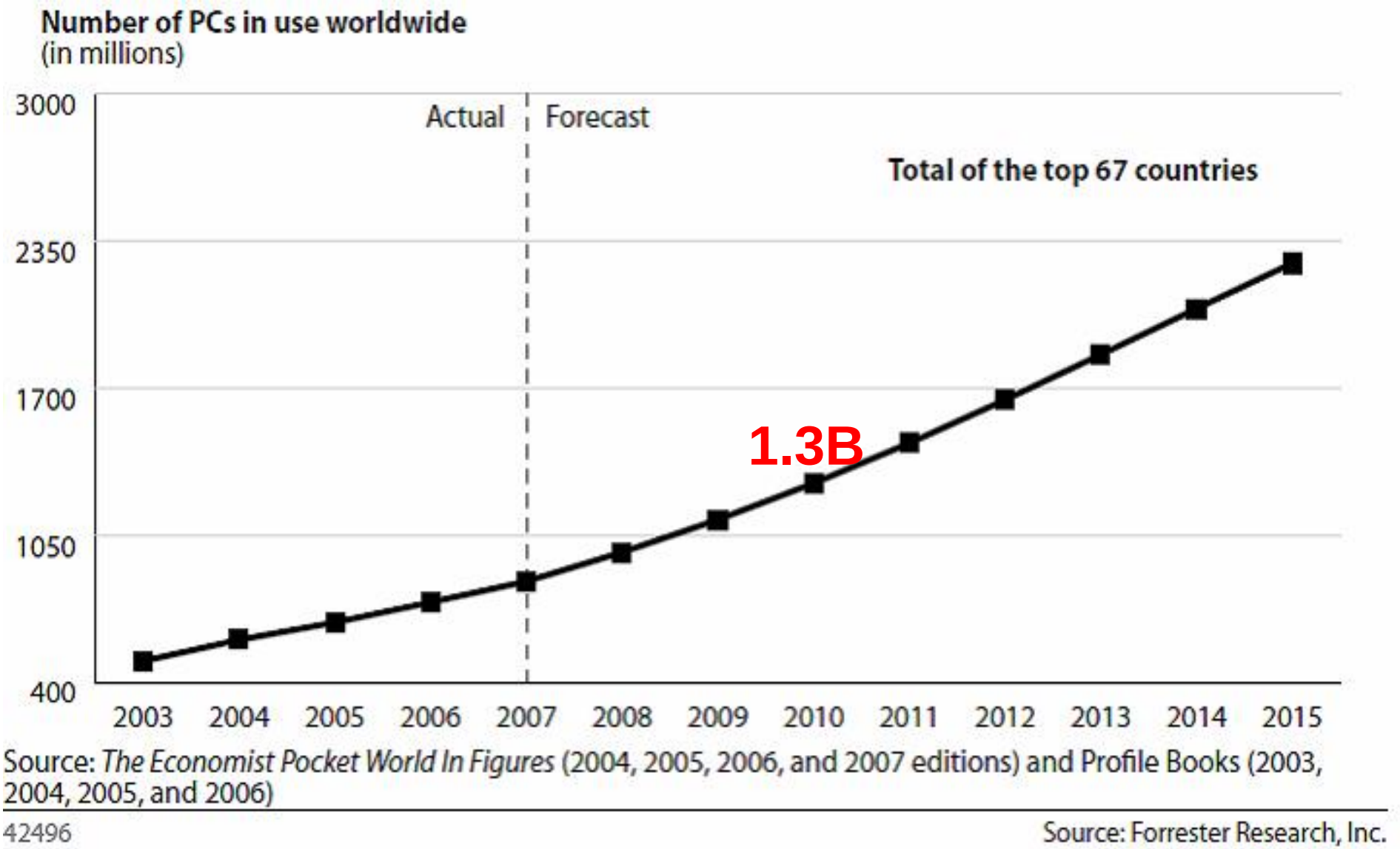
- **Democracy**
  - ICT presents opportunities and poses threats to democracy
    - Provide citizens with a wide range of information from a variety of sources
    - ICT threatens to undermine democracy by compounding existing biases in the distribution of knowledge and information
- **Crisis Prevention and Recovery**
  - One of the best examples is the Famine Early Warning System (FEWS) that has been established in Africa by USAID
- **Research, Environmental Observation and Management**

ICT & Broadband Diffusion – Figures and Facts

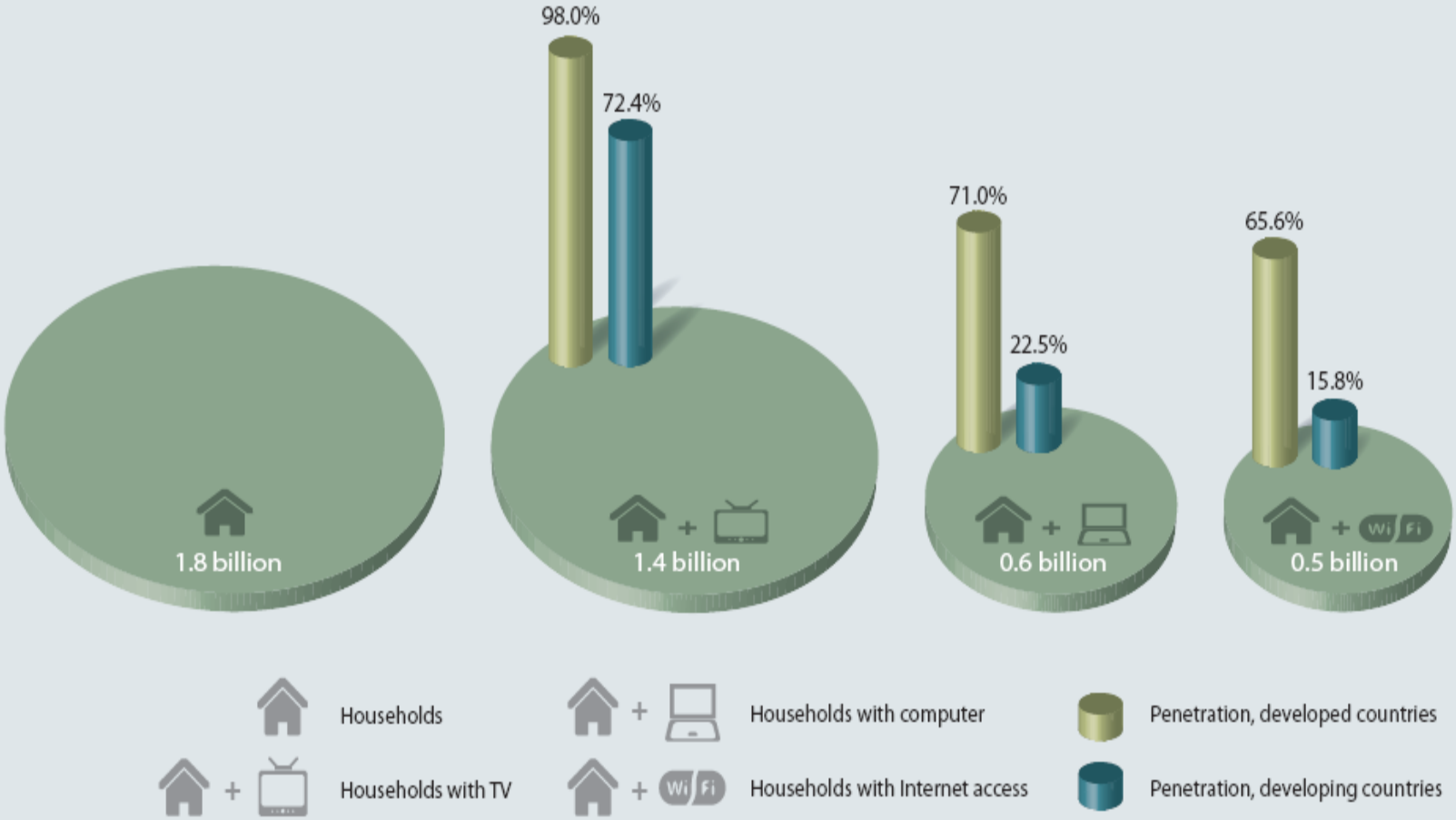
ICT Diffusion Global



PC Diffusion Global



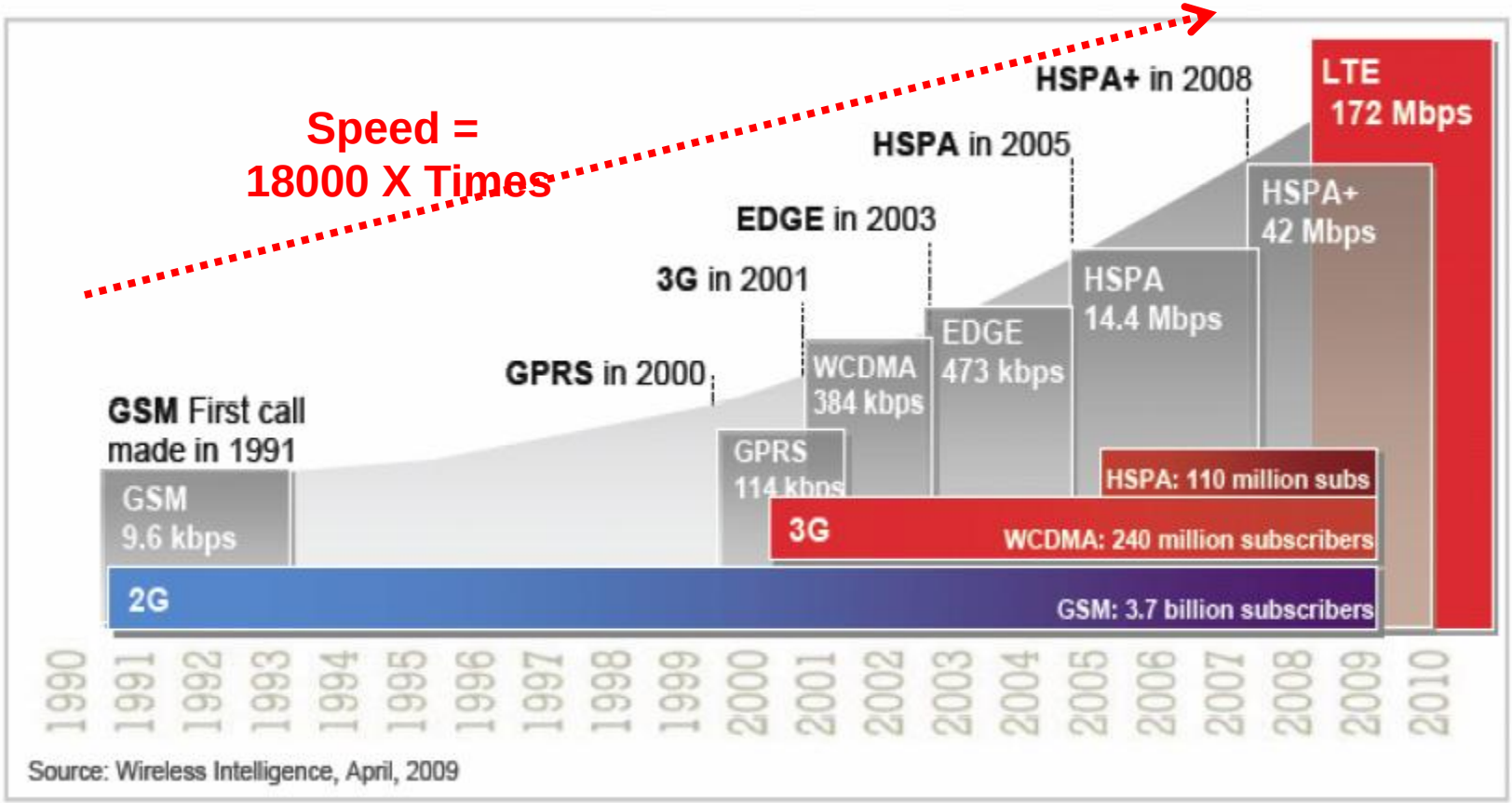
ICT Diffusion
Internet and Media Penetrations



Note: Data refer to 2010 and are estimates
Source: ITU World Telecommunication/ICT Indicators database

ICT Diffusion
Mobile Broadband

Evolution Path of 2G, 3G and 4G Technologies

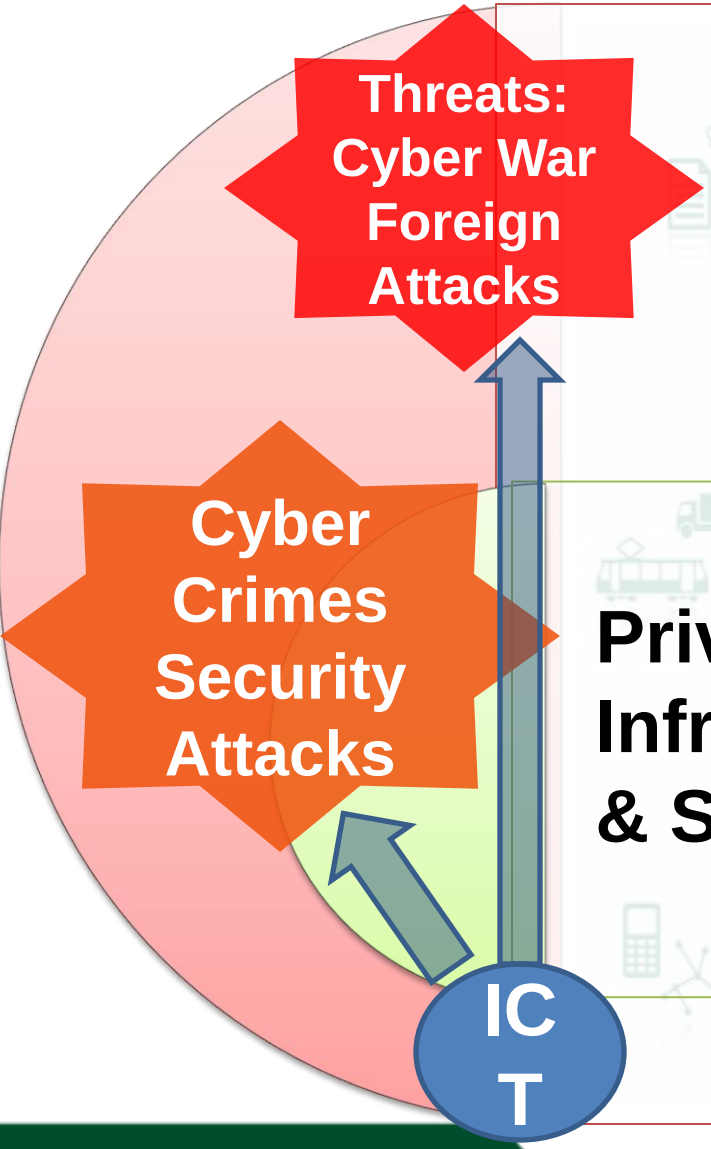


Source: Wireless Intelligence, April, 2009

HSPA+ peak theoretical data rate reaches up to 42 Mbps when using single carrier with QAM 64 and 2x2MIMO
LTE peak theoretical data rates reaches up to 172Mbps when using 20MHz channel and 2x2 MIMO

ICT Threats – Secondary Effects

ICT & Threats



Nationwide Public Infrastructures & Services

- **Civil**
- **Military**
- **Internal Security**

Private Infrastructures & Services

- **Economy, Finance & Business**
- **Education**
- **Health**
- **Social**
- **Personal use**

ICT & Threats:
Cyber War – A Science Fiction???

- Defined as "actions by a nation/state to penetrate another nation's computers or networks for the purposes of causing damage or disruption“

Richard A. Clarke, in his book Cyber War (May 2010),

Some facts:

- 2007: The Estonian Cyberwar
- 2008: Russian, South Ossetian, Georgian and Azerbaijani sites were attacked during the 2008 South Ossetia War
- 2010: Stuxnet, targeting many countries: India, Iran, China, etc…

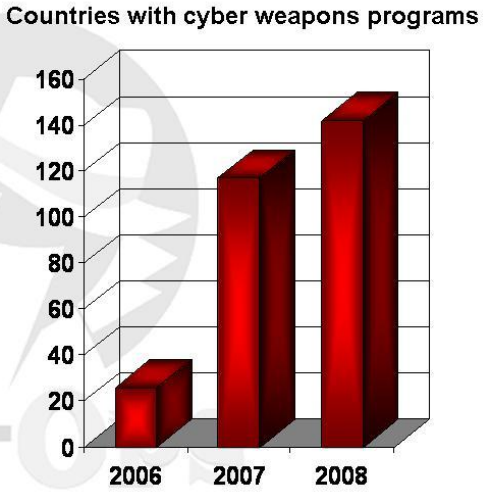
ICT & Threats: Cyber War …. A REALITY

INTELLIGENCE BRIEFING

Cyber Weapons Capabilities Growth

In one year, between 2006 and 2007, there was a substantial increase in the number of countries pursuing cyber weapons.

After analysis of available information, we have concluded that in 2008 there will be over 140 countries with cyber weapon programs.

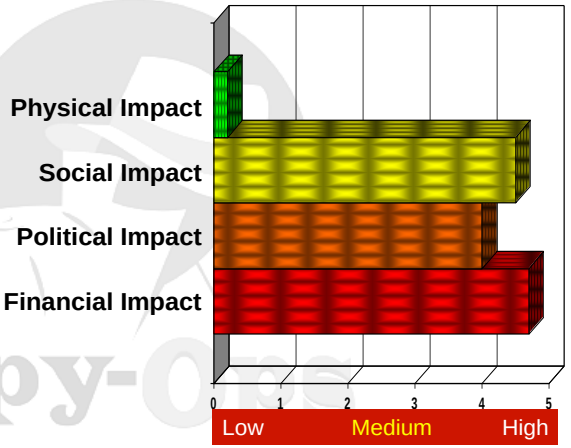


INTELLIGENCE BRIEFING

Impact of a Cyber War

The political fallout of a cyber attack will be high, but this will pale in comparison to the financial and economic impact!

The financial and economic impact could be as high as $30 billion a day!



www.Spy-Ops.com

2

- **Government involvement in Cyberwar in 2009**
  - **April:** The UK government confirms plans for a £2 billion tracking system to snoop network traffic for any criminal or dangerous activity, known as the Interception Modernization Program (IMP)
  - **June:** The US announces the formation of the US Cyber Command, an official military body dedicated to both defense against cyber-invasion and attacks against enemy computer networks
  - **November:** 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.
  - **Recently**, the existence of the unit 8200 within the Israeli intelligence dedicated for Cyber war and attacks, was revealed

ICT & Threats
Security Attacks

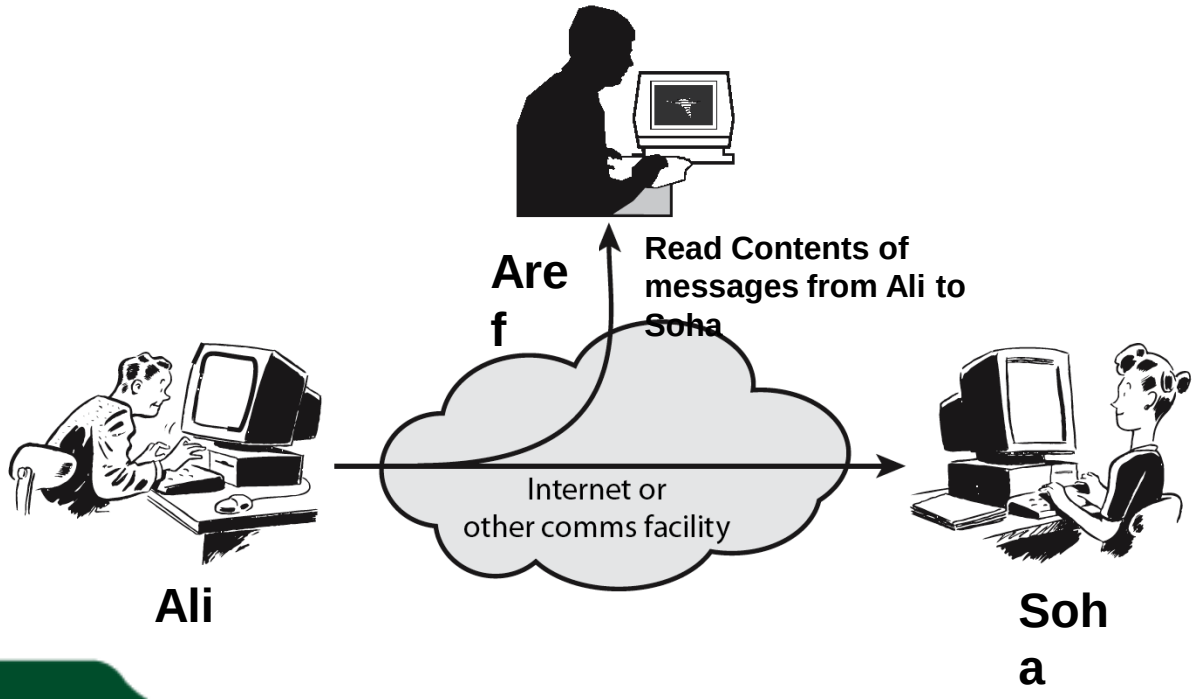
- Any action that compromises the information security
- Can be classified into two major categories:
  - Passive Attacks
    - Obtains data exchanged in the network without disrupting the operation of the communications
    - Examples of passive attacks
      - Eavesdropping, traffic analysis, and traffic monitoring.
  - Active Attacks
    - Involves information interruption, modification, or fabrication, thereby disrupting the normal network functionality
    - Examples of active attacks
      - jamming, impersonating, modification, denial of service (DoS), and message replay

Security Attacks Classification:

Passive Attacks	Eavesdropping, traffic analysis, monitoring
Active Attacks	Jamming, spoofing, modification, replaying, DoS

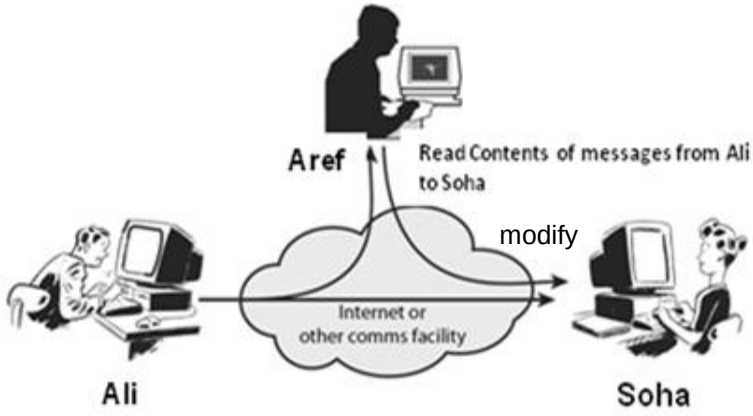
Security Attacks
Passive Attacks

- Attempt to receive, know, or make use of information from the system but does not affect system resources
- By eavesdropping on, or monitoring of, transmissions to:
  - Obtain message contents, or
  - Monitor traffic flows
- Are difficult to detect because they do not involve any alteration of the data



Security Attacks
Active Attacks

- Attempt to alter system resources or affect their operation
- Modify the data stream to:
  - masquerading one entity as some other
  - replay previous messages
  - modify messages in transit
  - denial of service
- "Man In The Middle" or "TCP Hijacking“
  - An active attack where the attacker sniffs packets, modifies them and inserts them back into the network
- Detection of Attacks
  - Passive Attacks are difficult to detect
    - Measures are available to prevent their success
  - Complete prevention of active attacks is quite difficult, because of the wide variety of potential physical, software and network vulnerabilities.
    - Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them



ICT & Threats - Security Attacks – Internet Relay Chat (IRC)-Based Botnet Works

1. Botmaster infects victim with bot worm, social engineering, etc)

Hi, want free MP3 songs? Click this link!
HTTP://mmmeasy.com ==> **Bot downloaded**

2. Bot connects to IRC C&C channel

Botmaster

Bots$_{1,2,3,..}$

Victim

3. Botmaster sends commands through IRC C&C channel to bots

Bot…n

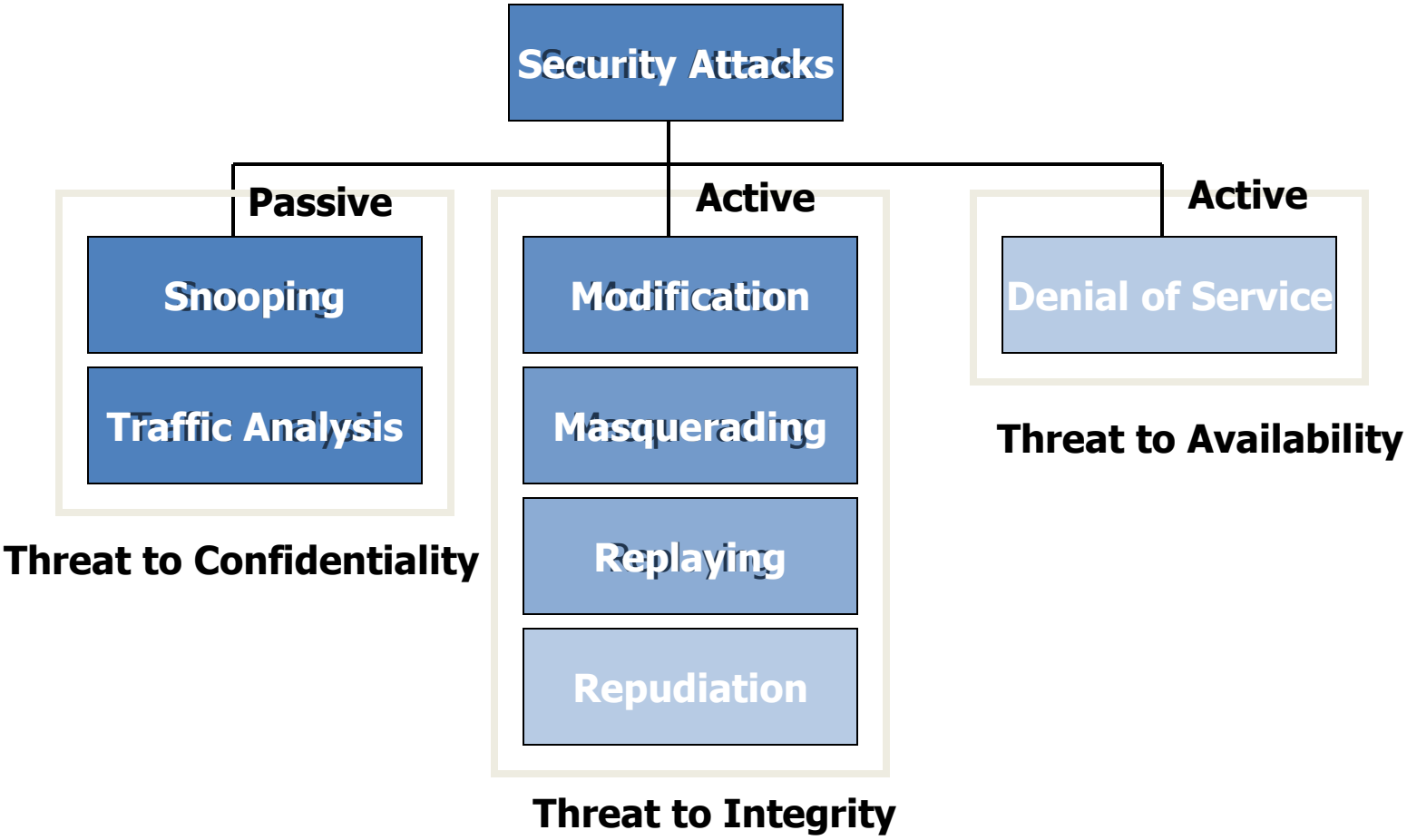
4. Repeat. Repeat>

Soon the botmaster has an army of bots to control from a single point

Bots, freeze the server!

IRC Server (Undernet, EFNET, etc…)

Examples of Security Attacks



ICT Security - ITU Framework

Information Security - Definition

Information Security***:*** *Protecting information & information systems from unauthorized:*

- *Access*
- *Use*
- *Disclosure*
- *Disruption*
- *Modification*
- *Perusal*
- *Inspection*
- *Recording & Wiretapping*
- *Destruction*

- Many Specialization Areas
  - Securing networks and related infrastructure
  - Securing applications, databases,…

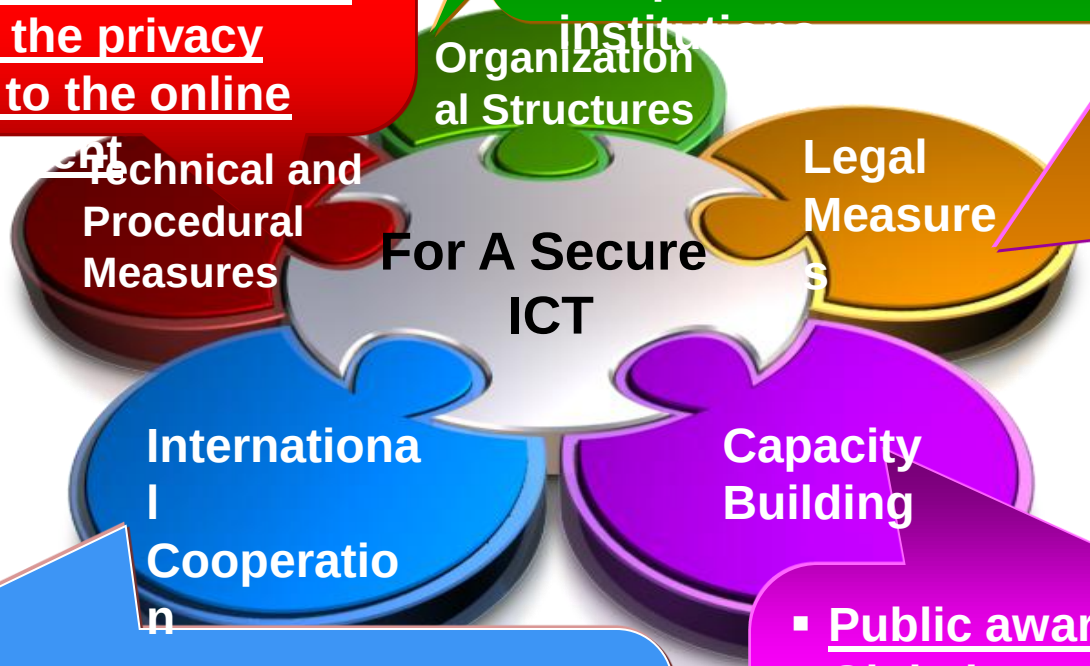
ICT Security

- Information security challenges must be met with a combination of factors: **People**, **Organizations**, **Processes**, **Laws** & **Regulations**, and T**echnology**
  - Individuals must be vigilant in maintaining the security processes laid out by the organization
  - Organizations must implement and enforce security processes and procedures
  - Businesses and Government must use multiple layers of security technology to deter threats and must go through international cooperation

Steps Towards Developing a Culture of ICT Security (Based on ITU framework)

- Global framework for security protocols, standards, S/W, H/W, & accreditation schemes
- Update the privacy regime to the online

- Global strategies for national and regional organizational structures and policies
- Cooperation between all



- National policy awareness
- Harmonization of legal frameworks
- Cooperation with other elements of the national cyber security I/S & private sector

- Enhance international dialogue on cyber security issues and enhance cooperation and coordination
- Participate in international efforts

- Public awareness and education
- Global strategies to facilitate human and institutional capacity building
- Training for criminal justice professionals
- Encourage the private sector to

ICT Security : Technical Measures
Securing Infrastructures - ISO27k Standards

- ISO/IEC 27k- Information Security Standards
  - Standards provide generally-accepted good practice guidance on Information Security Management Systems (ISMS) designed to protect the confidentiality, integrity and availability of the information content and information systems
- Four ISO27k standards are already available
  - ISO/IEC 27001 - the ISMS certification standard
  - ISO/IEC 27002 - the code of practice for information security management with advice on a broad range of controls
  - ISO/IEC 27005 - with advice on information security risk management
  - ISO/IEC 27006 - a guide to the ISMS certification process for certification bodies

Security Goals

- **Confidentiality (Privacy)**
  - Protection of data from unauthorized disclosure, information is available for authorized parties only
- **Integrity**
  - Assurance that data received is as sent by an authorized entity, unauthorized parties can not modify information
- **Authentication**
  - Peer authentication and data origin authentication
  - Assurance of the identity of a peer entity and the origin of information
- **Availability**
  - Ensure resources or communications are not prevented from access by Denial of Service (DoS) attacks
- **Non-repudiation**
  - Protection against denial, an entity can not later on falsely deny a valid transaction
- **Access control**
  - Prevents unauthorized access, unauthorized persons can not access resources

Security Solutions

- Security can be ensured by protocols, software, access control, encryption, etc..
- Integrity and availability of the information
  - Ensured using authentication and authorization processes
- Confidentiality of messages
  - Most important problem especially in an open wireless medium
  - One possible solution is “Cryptography”

Access Control
Authentication, Authorization, Accounting (AAA)

- AAA is a model for access control
  - Authentication
    - Determining whether a user should be allowed to access a system or a resource
  - Authorization
    - Concerned with restrictions on the actions of authenticated users, “what the user is authorized to do?”
    - Administrator accounts and Firewalls
  - Accounting
    - Is keeping track of what the user does
- Multilevel securitv labels the information as:

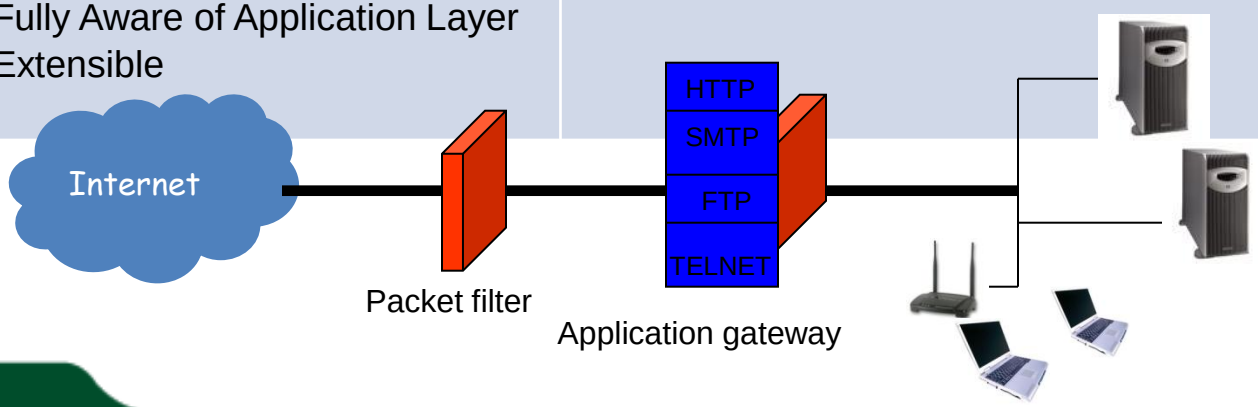
  TOP SECRET > SECRET > CONFIDENTIAL > UNCLASSIFIED.

  - Using this categorization, the user can only reach information of appropriate class

ICT Security : Technical Measures
Firewalls

- The Firewall/DMZ Environment
  - Firewall is designed to block unauthorized access while permitting authorized communications

Firewall Solution	PROS	CONS
Packet Filters	• Application Independent • High Performance • Scalable	• Low Security • No Protection Above Network Layer
Application-Proxy Gateways	• Good Security • Fully Aware of Application Layer	• Poor Performance • Limited Application Support • Poor Scalability
Stateful Inspection	• Good Security • High Performance • Scalable • Fully Aware of Application Layer • Extensible	• More Expensive



ICT Security : Technical Measures
Intrusion Detection Systems (IDS)

- Intrusion Detection System (IDS)

  Monitors network and/or system activities for malicious activities and produces reports to a Management Station

  – **Network IDS** can be integrated with firewalls to automatically respond to attacks

  – **Host-based IDS** can detect changes to operating system programs and configurations

Cryptography/Encryption

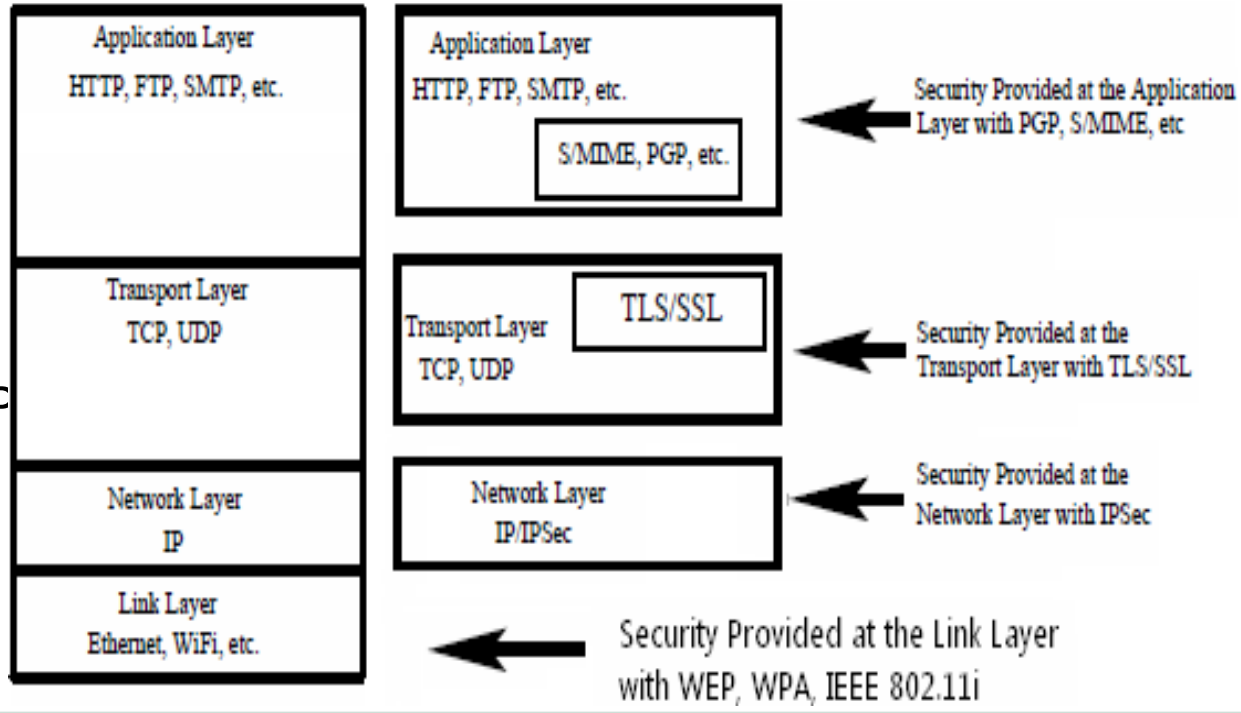
- **Cryptography**
  - **Transforms usable information into a form that renders it unusable by anyone other than an authorized user**

  - *Encryption functions take at least two inputs: The **Plaintext** , and the **Encryption Key** (sometimes referred to as keying material)*

- Encryption Techniques
  - Symmetric Encryption (Secret Key Encryption)
    - Symmetric algorithms: DES (Data Encryption Standard), 3DES (Triple-DES), AES (Advanced Encryption Standard)
  - Asymmetric Encryption (Public Key Encryption)
    - Asymmetric algorithms: RSA (Rivest, Shamir and Adleman), DSA (Digital Signature Algorithm), PGP (Pretty Good Privacy)

Security Protocols

- Security may be provided at different layers
  - Secure network-based applications
    - Web – **SSL/TLS**, transport layer solution
    - Email – **PGP**, application layer solution
  - Secure network + support for application
    - **IPSec** for network layer security
    - Internet Security
      - BGP security (**S-BGP**)
    - Wireless Security
      - IEEE 802.11: WEP, WPA, WP



Wireless Security

- Wireless Equivalent Privacy (WEP)
  - A link-level security mechanism defined in IEEE 802.11
  - Stream cipher RC4 is used in a nonstandard way
  - CRC checksum is used for integrity protection
  - Problems with WEP
    - WEP is a weak encryption algorithm, WEP encryption can be cracked today in an average of 10 minutes
- Wi-Fi Protected Access (WPA)
  - An intermediate solution to address WEP's problems while WPA2 is the longer-term solution
  - WPA introduced new authentication protocol, improved integrity protection measure and per-packet keys

Additional Techniques Used in IT Security

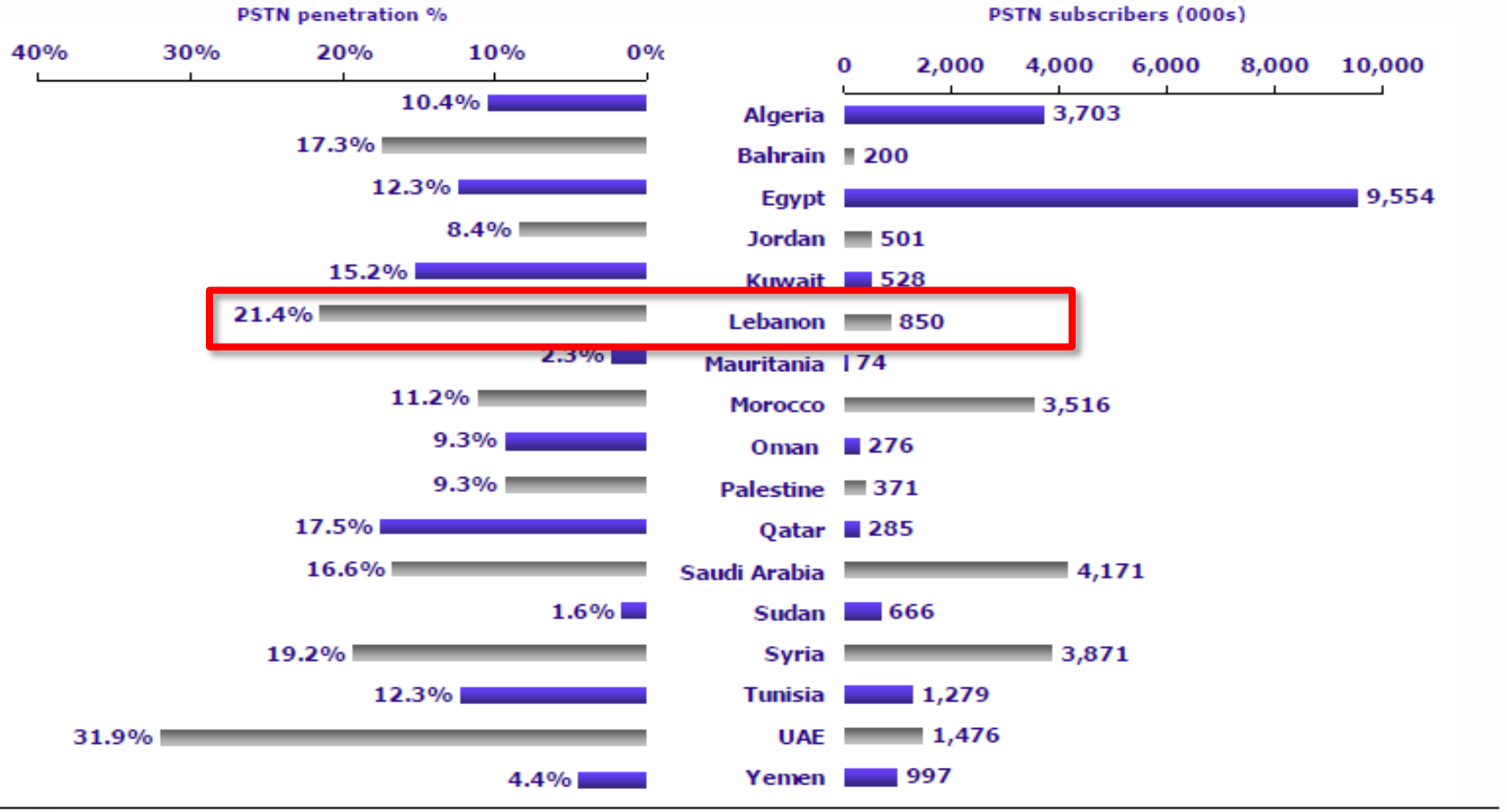
- **Browser Virtualization**
  - **Execute only the system components necessary for the chosen browser**
- **Managed Security**
  - **Offloading firewalls and intrusion detection/prevention to a third party**
- **Cloud Security**
  - **Cloud security products work by blocking attacks and spam in the cloud, before reaching the enterprise network**
- **Cloud Firewalls**
  - **Augment (not replace) enterprise firewalls/IDS by dealing with big threats**
- **Next Generation Firewalls**
  - **Firewalls that provide full layer-7 awareness**
- **Cloud Computing**
  - **Access control and identity management become essential to secure data and who has access to it**

NOTE: Specialized Data Centers /Cloud Computing Provide a major advantage over personal security

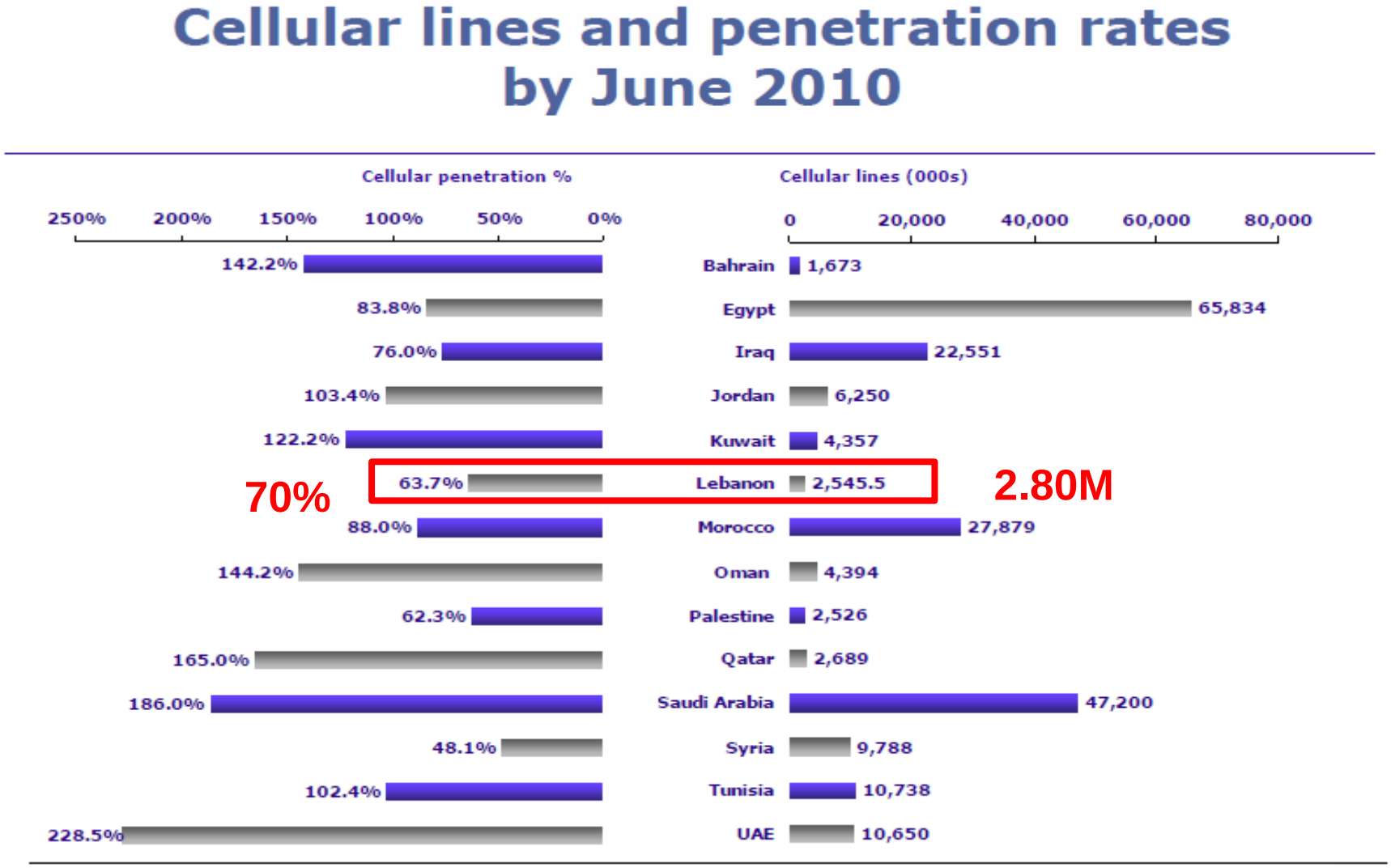
ICT Security - Lebanese Case

Lebanese Case
Selected ICT Figures - Arab Fixed Lines

17 Arab countries had 32.3 million fixed lines by end of 2009

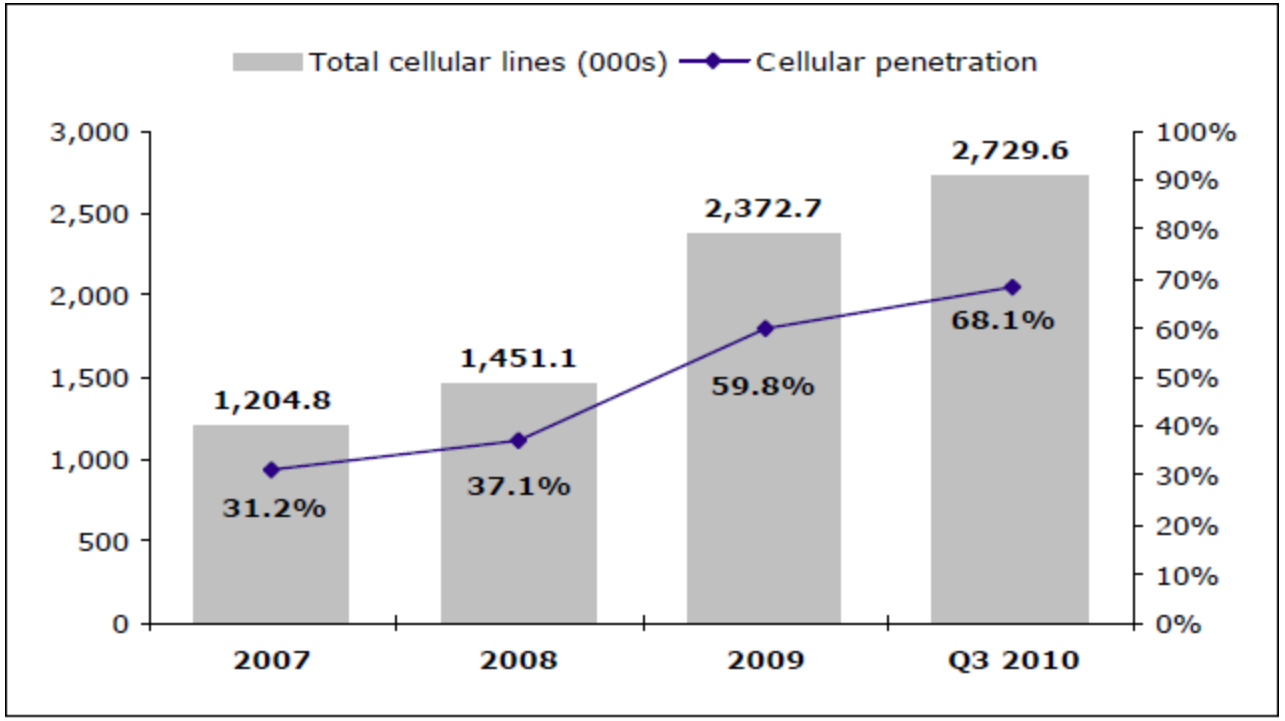


Selected ICT Figures - Arab Cellular Lines



Lebanese Case

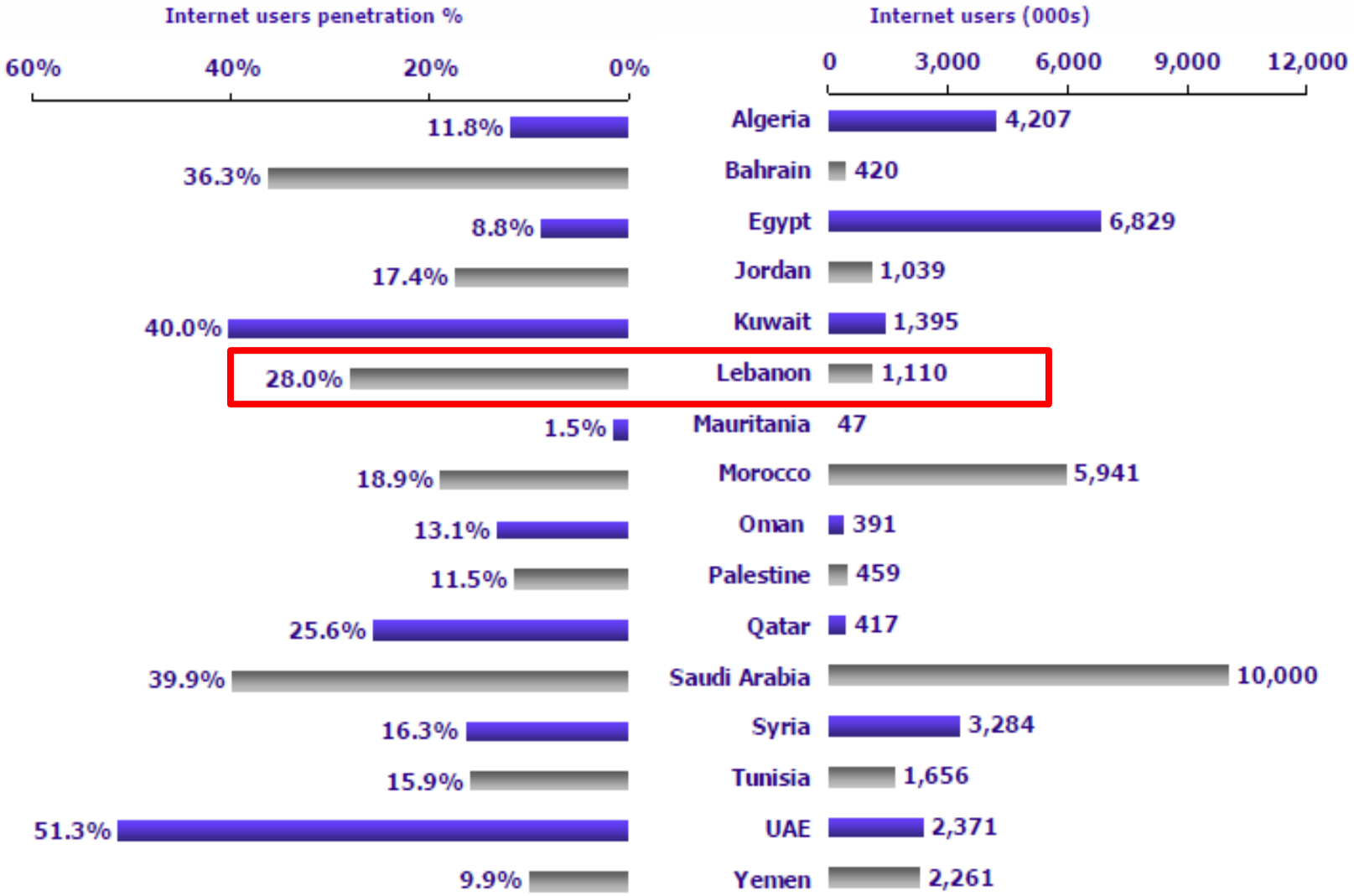
Selected ICT Figures - Lebanese Cellular Lines



* Based on Arab Advisors Group estimated population for Lebanon.

Source: MTC Touch, Alfa, Arab Advisors Group

Lebanese Case
Selected ICT Figures - Arab Internet Users



Cyber Crimes Stats – 2010 (Cyber Crime Office)

Nature of Attack	Number of incidents	%
• Threat of Reputation Abuse, Extortion and Defamation via Internet / Phone	285	56%
• Theft of Electronic Account and Use it for Criminal Purposes	92	18%
• Online Fraud and Impersonating ID's	48	9.8 %
• Disturb and Bullying over the Internet / Phone	27	5.35 %
• Theft and Use of Stolen e-mail	8	1.6 %
• Credit Card Fraud	8	1.6 %
• Falsification of Touristic Sites and Disseminate them via Internet	4	0.8 %
• Online Gambling Games	11	2.18 %
• Money Embezzlement and Bank Accounts Fraud	4	0.8 %
• Fraud of Telephone Calls	2	0.4 %
• Software Piracy and Theft of Programs & Designs	1	0.2 %
• Sexual Exploitation of Children Online	14	2.8 %
Total:	504	

Lebanese Case
Characteristics of the ICT Sector - Piracy

- According to International Data Corporation (IDC), the piracy rate in Lebanon
  - was stable at 73% during the years 2003–2008
  - reached 74% in 2008
  - returned to 72% in 2009
- In 2009, the value of annual losses experienced by companies producing software are estimated at $49M
- IDC also estimates that if the piracy rate for software in Lebanon decreases by 10% points over the 4 years, then this will lead to:
  - The creation 300 additional job posts in the ICT sectors
  - The ICT local sector will benefits from additional incomes exceeding $27 million (+$3M in additional tax revenue for the treasury)
  - The increase of the contribution of the ICT sector by more than $50M to the overall national income

Lebanese Case
Selected ICT Figures

Benefits from Reduced Piracy: Lebanon

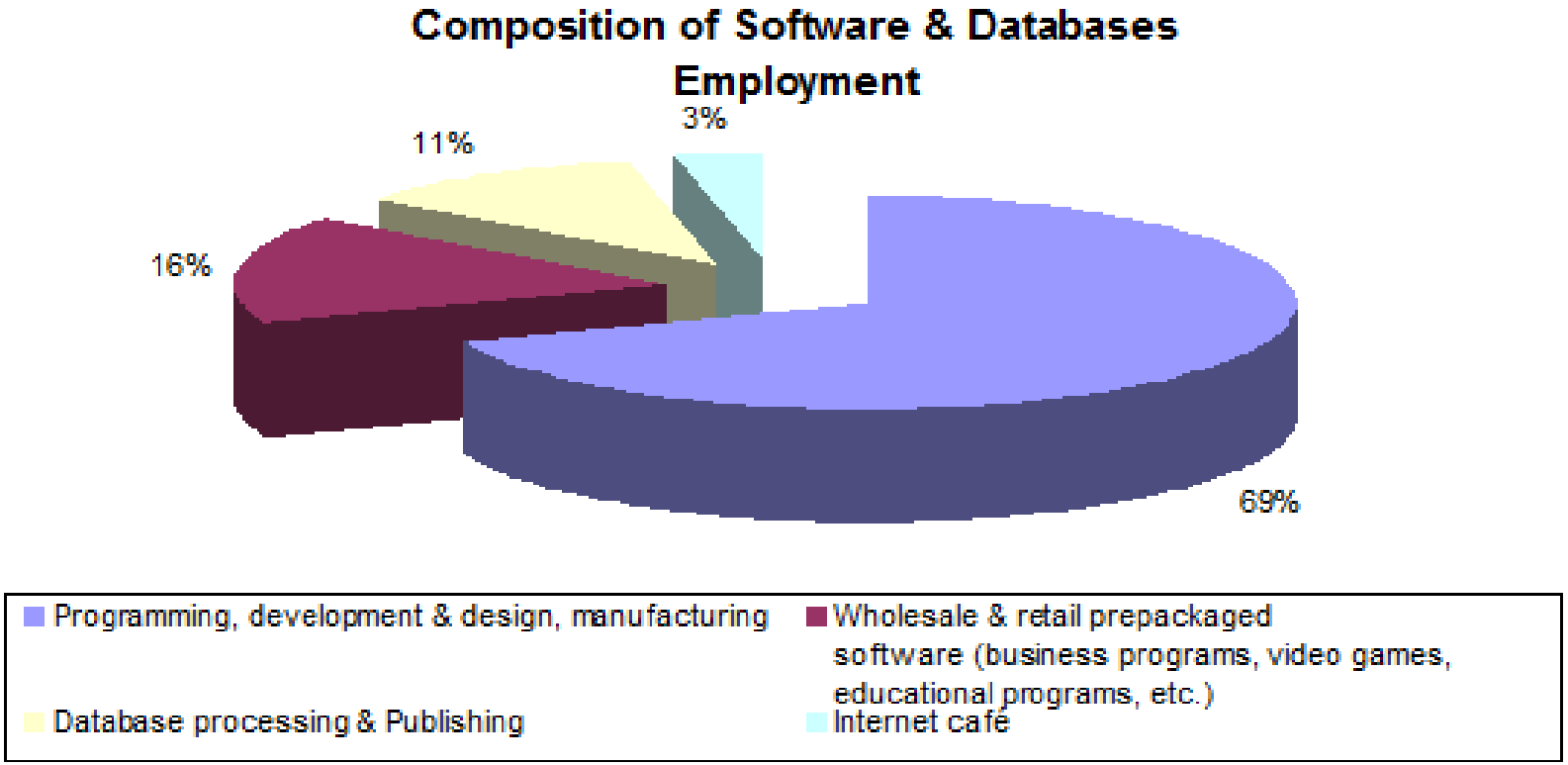
Impact	Cut in Piracy Rate	
	10 Percentage Points	12 Percentage Points
% Per Year, 2010–2013	2.5	3.0
Contribution to GDP (US$M)	$51.92	$56.70
Additional Local IT Revenues (US$M)	$27.11	$29.61
New Jobs	314	343
Additional Tax Revenue (US$M)	$3.43	$3.75

Source: IDC Economic Impact Study, 2009

Lebanese Case
Selected ICT Figures - Spending on IT in Lebanon

- In 2008, IT expenditure in Lebanon was around $350M
  - Growth of 20% over last year
- Distribution of this spending:
  - 77.3% on equipment and supplies
  - 12.8% of the services sector
  - 9.9% on software
- It is expected that IT spending in Lebanon in 2013 to reach nearly $500M

Lebanese Case
Selected ICT Figures – S/W and DB Employment



- **The sector consists of 527 operators, employing 2,456 workers and contribute around 0.22 percent to overall employment**

Source: WIPO Study on the Economic Contribution of the Copyright Industry i

Lebanese Case
Characteristics of S/W and DB Corporations

The **IT sector** in Lebanon consists of about

- 527 companies/foundations
- 374 of them are working in the software & programming field
- 5 big companies are estimated to control about 50% of the market
- A large number of companies do not survive their first year
- Most companies are located in Greater Beirut and Mount Lebanon areas
- The level of services varies largely between these companies, ranging from offering high-quality services at a global level, to poor services provided by weak companies
- The contribution of this sub-sector to the GDP is equivalent of 0.39%
- According to a study by the **"World Intellectual Property Organization"**, the sector contributes about $329.7M (1.1% of GDP), including $85.13M in added value

Lebanese Case
Selected ICT Figures

TABLE 1

IT Profile and Forecast: Lebanon

	2008	2009	2010	2011	2012	2013	CAGR (%)
Spending (US$M)							
IT Hardware	254.77	235.03	275.22	317.91	362.74	403.94	9.7%
Software	42.24	43.72	47.66	52.49	58.79	66.13	9.4%
IT Services	32.74	33.28	35.04	38.02	41.71	46.28	7.2%
Total IT	329.75	312.03	357.93	408.43	463.25	516.36	9.4%
IT Contribution							
IT/GDP (%)	1.1%	1.0%	1.1%	1.1%	1.2%	1.3%	
IT Tax Revenues (Million LBP)	23.08	22.86	26.01	29.93	33.42	37.00	9.9%
Total Number of IT Companies	826	824	866	914	969	1,025	4.4%
IT Employment							
Total Number of Employees	8,651	8,586	9,218	9,956	10,789	11,662	6.2%
Total Software-Related Employees	2,890	3,279	3,356	3,510	3,758	4,093	7.2%

Source: IDC Economic Impact Study, 2009

Current Lebanon's Legal Framework Is ICT Secure?

- **Law on the Protection of "Intellectual Property Rights (IPR)" -No. 75 / 1999**, partially addresses the issue of piracy of computer programs - Articles 83 to 89
- **Central Bank of Lebanon Regulations (March 2000) and Declarations (July 2000)** for the safety of IT issued to regulate the electronic banking, setting out the protection measures to be followed by banks and financial institutions
  - Designates **responsibility** for of the safety of information technology
    - a general committee
    - a person in each institution
  - **Terms for staff accessing the information systems**
  - **Fundamentals of safety** management of information technology
  - **Terms of communication systems and computer hardware and safety system of devices and centers**
  - **Emergency plans and the resumption of work**
- **Draft E-Transaction Law** in the parliament – Does not address the need
- **No coordination yet between the public and the private sectors** on the issues related to the networks and information protection – there is a Pan Arab Forum
- **Lebanon has no legislation(s) related to ICT Security**
- **Cyber Security Effort is moving slowly**

Lebanon Case Study
Security Risks in the WLAN (MORE VULNERABLE)

Non-secure WLANs can expose an organization's network traffic and resources to unauthorized outsiders, that

- capture data and exploit network-based resources, including Internet access, fax servers, and disk storage

- **Data Confidentiality**
  - Data is exchanged through clear air, thus unauthorized people can easily listen and read it. This can have severe impact if data contains personal and business information
- **User Privacy**
  - Personal and business information can be used as a hint by hackers for direct attack
- **Unauthorized Internet Access**
  - When the Access Point (AP) broadcasting its SSID name and doesn't filter legitimate clients

Possible Solutions
Several Measures Can Be Used to Secure WLANs

- **Develop a WLAN Security Policy**
  - to define access to the network, and services and encryption of data
- **Management Frame Protection (MFP) and Wireless IDS**
  - Protect the network from external sources and devices not controlled by infrastructure
- **Protection of the WLAN Devices and Managed User/Device Connectivity**
  - Authentication framework to facilitate authentication messages between clients, AP and AAA server
  - Authentication and Encryption algorithms— to validate client credentials and provide data privacy
    - Use strong encryption methods like WPA-PSK and avoid using the weak WEP encryption
  - Message integrity - ensures data frames are tamper free and truly originate from the source address
  - Using MAC filtering to grant access for only known clients
- **Firewall Integration**
  - Fully featured, highly scalable firewalls for enhanced policy enforcement

Current Facts- Threats On PSTN (FIXED) Network

1. Intercepting the MW network connectivity
2. Accessing the Network Operation Center (NOC) via VPN-Internet Connection
3. Changing/creating pre-programmed links to phone numbers on the fixed network using the same specs as the base number
4. Changing/creating direct Physical Connection links from the Main Distribution Frame (MDF) to allow use of, and tapping
5. Breaching the management elements and systems, including the billing system, by exploiting the remote control feature available for maintenance
6. Accessing security systems in the fixed telecom networks through backdoors to access to the systems of such networks
7. Using the signaling network SS7 to infiltrate the components of the PSTN network by introducing a microwave link with a small antenna facing the antenna of the third party

Lebanon Case Study
Possible Security Risks in GSM Networks

Operation & Management Center (OMC)

Mobile Switching Center (MSC)

Mobile Switching Center (MSC)

Gateway Mobile Switching Center (GMSC)

Other Centers

AUC

HLR

VLR

Base Station Controller (BSC)

Base Station Controller (BSC)

(PSTN)

Base Transceiver Station (BTS)

Base Transceiver Station (BTS)

1 2 3 4 5 6 7 8

Lebanon Case Study
Security Risks in GSM Networks

- **Unable to detect Active Attacks**
  - Impersonating network elements such as false BTS is possible
- **Security Key Transmission**
  - Cipher keys and authentication values are transmitted in clear within and between networks (IMSI, RAND, SRES, Kc)
- **GSM Encryption uses A5 algorithm** for both voice and signaling data
  - Is used only between the handset and the BTS
  - Is vulnerable to generic pre-computation attacks and the A5 encryption can be broken easily
- **Channel Hijacking**
  - Protection against radio channel hijacking relies on encryption
  - However, encryption is not used in some networks
- **GSM Authentication: A3 is the "MS authentication algorithm" and A8 is the "Voice-Privacy key generation algorithm" in the GSM security model**
  - Unilateral Authentication: only user is authenticated, no means to identify the network to the user. This makes the network vulnerable to man-in-the-middle attacks
  - A8 algorithm can be cracked easily by retrieving the secret key as the RAND and SRES are sent in plain text. Such vulnerability undermines the security of the whole GSM Network
- **Inflexibility**
  - Inadequate flexibility to upgrade and improve security functionality over time

Lebanon Case Study
Current Facts- Threats On GSM

1. Breaching the SIM card security
2. Decrypting the encryption codes
3. Eavesdropping on all calls using MW links (not encrypted)
4. Accessing the support systems
5. Downloading programs on network components through the OMC
6. Installing equipment at BTS locations
7. Making fake calls either directly or remotely
8. Accessing the SS7 signaling network by introducing MW links and antennas
9. Re-configuring the MW links protection system
10. Using repeaters to increase the coverage of base stations
11. Accessing the main links of the GPRS Network
12. Penetrating supplier companies
13. Accessing the security systems through dedicated backdoors
14. Impersonating a of a cellular number (Cloning)
15. Implanting a full programmed SIM card (IMSI + IMEI)

Current Threats- Effects Summary

1. **Controlling** the networks (cellular or landline) and its components
2. **Disabling** parts, (or all) of the network / isolating users
3. **Locating** people and tracking their movements and defining the pattern of their moves and contacts
4. **Eavesdropping** on voice calls, accessing message content, and eavesdropping on the surrounding
5. **Making fake calls and messages**
6. **Collecting the detailed records** (caller, called person, locations, devices, time and duration of communication)
7. **Adding/eliminating/modifying data**
8. **Manipulating user's cellular elements** – SIM Card and the device
9. **Broadcasting** voice and written messages

BLACKBERRY CASE

Highlights of the Security Actions PLAN

1. Issue sector policy and restructure the sector
2. Establish and implement procedures for selecting suppliers, operators, staff & experts
3. Establish and implement procedures for the selection and admittance of telecom equipment and devices
4. Establish and implement procedures to ensure and audit the safety and security of telecom networks
5. Establish and implement procedures for checking the conformity of planning, management, operation and maintenance of the network with security standards
6. Establish and implement procedures for dealing with border infringements
7. Separate military/security communications networks from the civilian one
8. Enhance the contribution within the ITU
9. Establish and implement measures to protect consumers & personal data

Thanks

Շնորհակալություն

www.tra.gov.lb