Republic of Lebanon
Telecommunications
Regulatory Authority

Cyber Threats and security efforts Broadband considerations

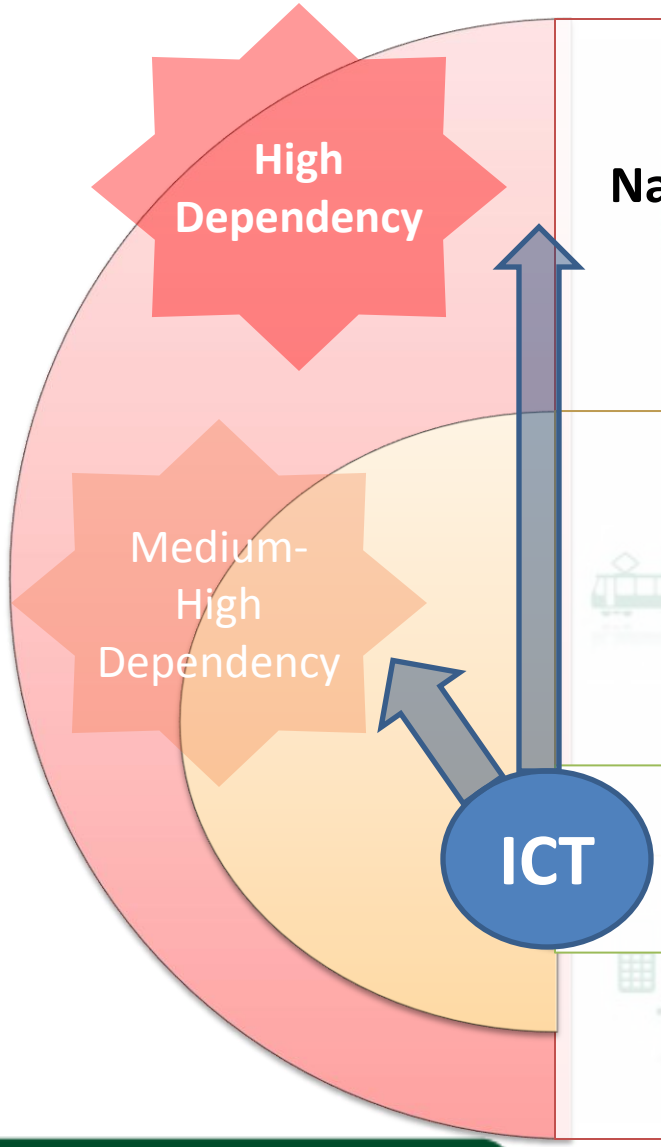
Said Haidar
Type Approval, QoS and Standards Manager,
Telecommunications Regulatory Authority (TRA), Lebanon

Agenda

- Role of ICT in Contemporary nations
- ICT & broadband diffusion – Figures and facts
- Cyber Threats – per kind & per sector
- Teens & ICT – threats and measures
- Cyber security – Measures, efforts & solutions

Role of ICT – Nationwide degree of dependency

ICT & National Resources



Nationwide Basic services

- **Civil:** Energy, Communications, Water supply & drainage, transportations, etc…
- **Military:** Command & Control, Intelligence, defense, etc…
- **Internal security**: Investigation & Forensics, Emergency, etc…

Sector Specific

- **Economy & business**: Industry, Banking, E-commerce, agriculture, etc…
- **Education**: E-learning, E-libraries, etc…
- **Health**: Tele-health, assisted Surgery, etc…
- **Social**: Global literacy, capacity building, rights to access information (Personal information & Children online issues), etc…

- **Fixed & Mobile Infrastructures**
- **Internet Capacity & access**
- **Computers & IT applications & Media & RTTEs**

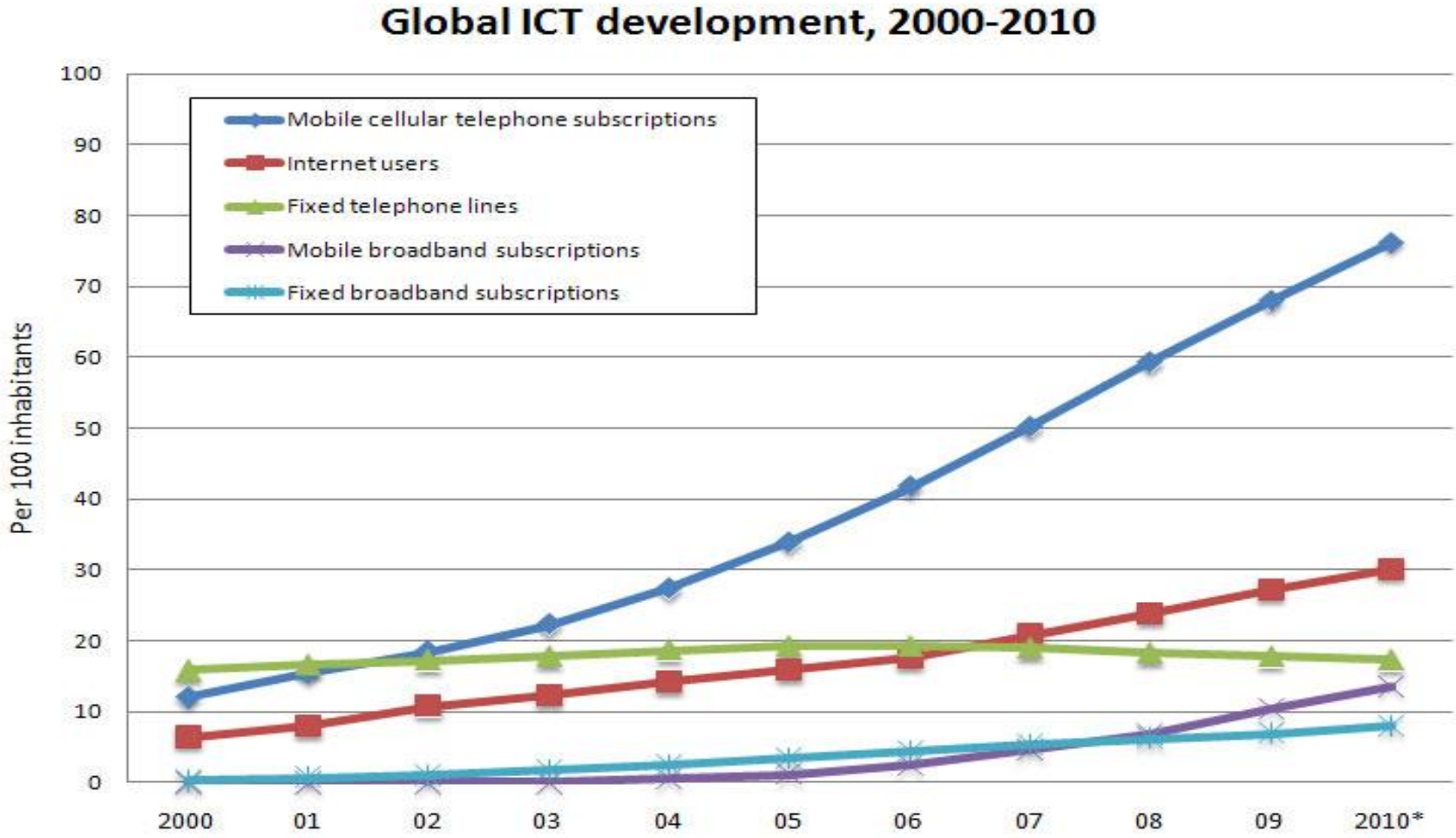
ICT & developing world
Benefits

- **Economic productivity and infrastructure development**
- **Health and the Fight against Disease**
- **Education and learning**
- **Poverty alleviation**

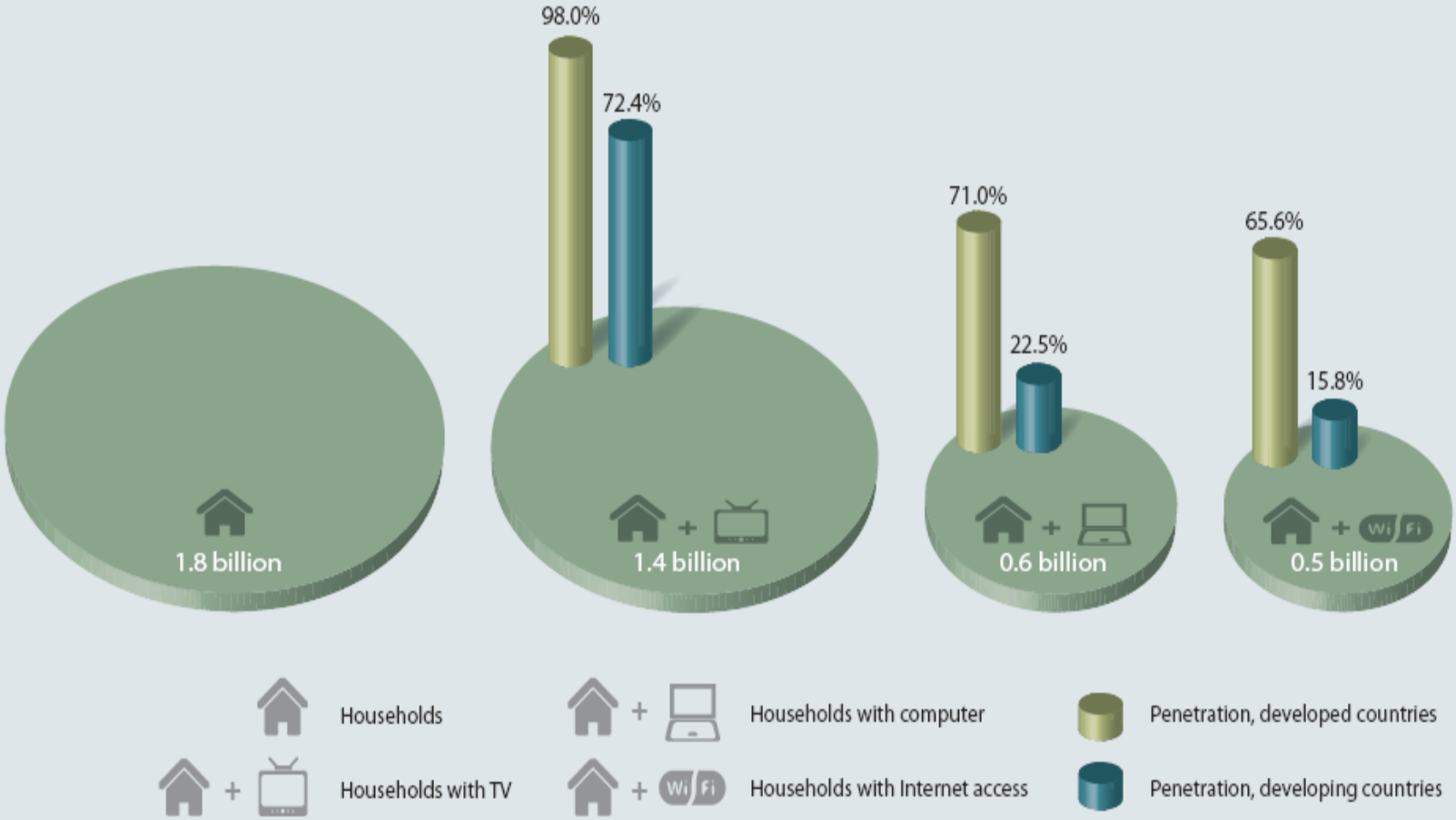
  "Village Internet Program of the Grameen Bank in Bangladesh aims to promote poverty alleviation by reducing migration from villages to cities, and creating IT-related job opportunities for the rural population" (Grameen Bank, 1998).
- **Empowerment of marginalized groups**
- **Sustainable development & awareness**

ICT & Broadband diffusion – latest Figures and facts

ICT diffusion
Global

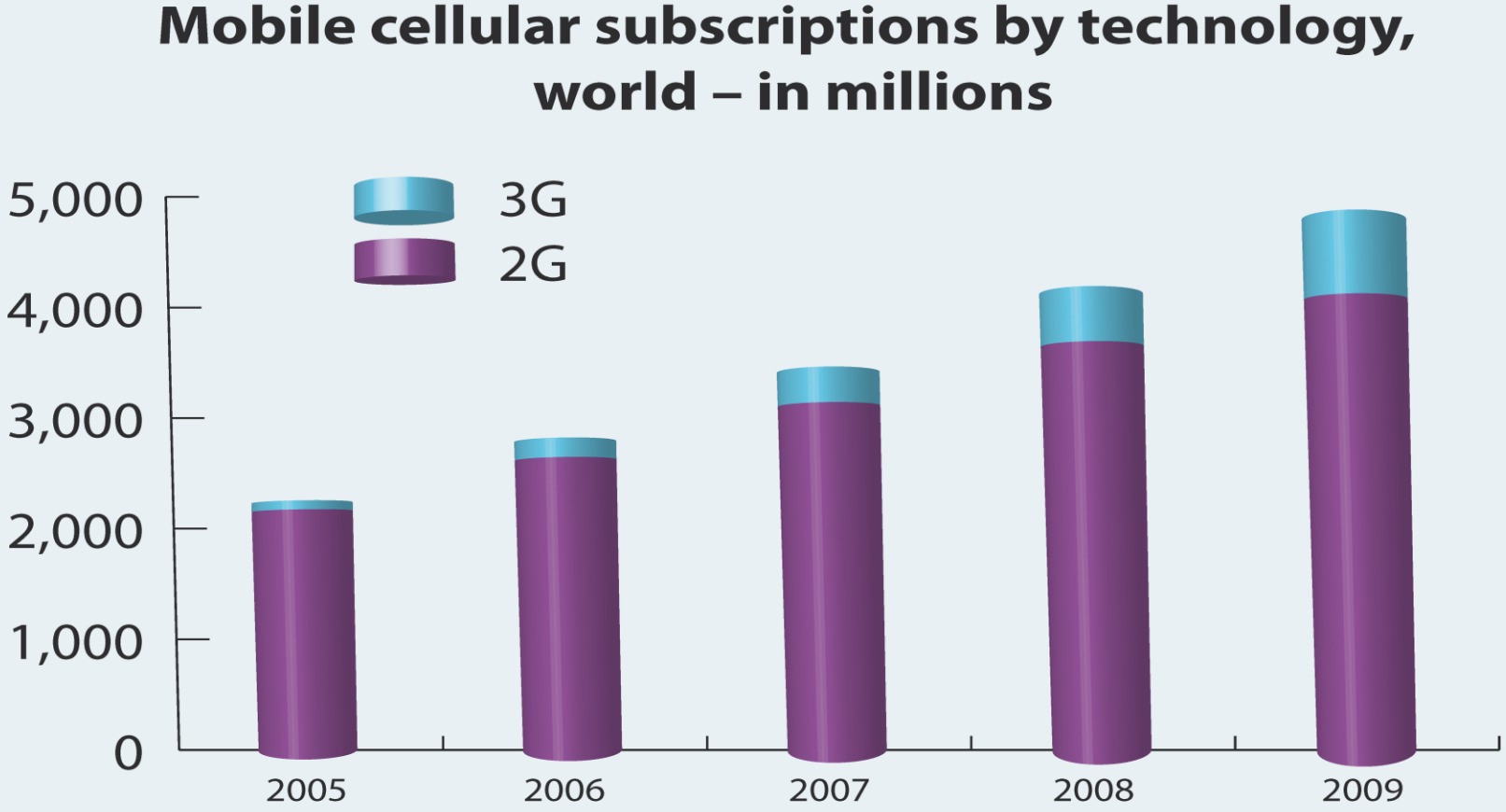


ICT diffusion
Internet and media penetrations



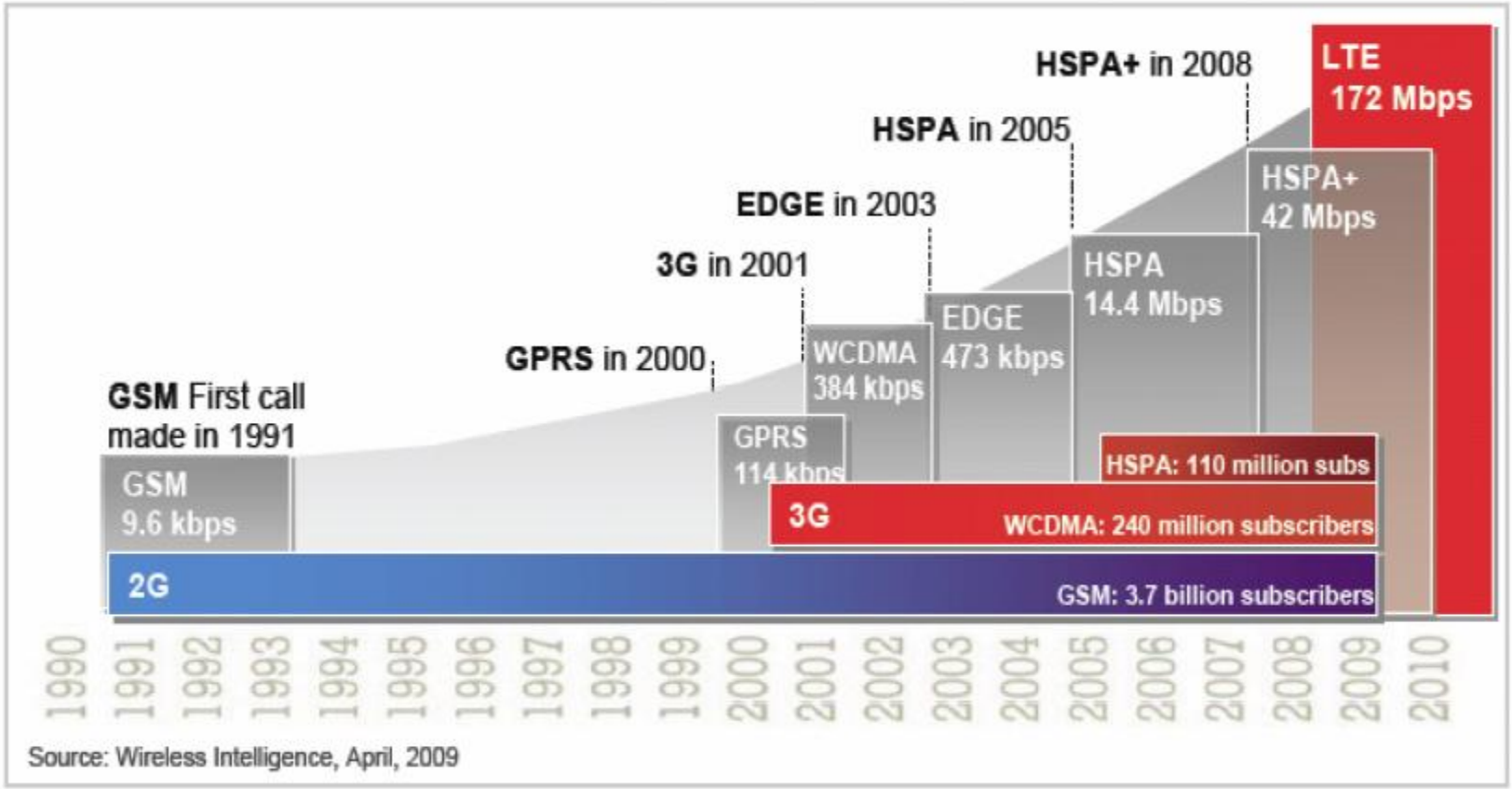
Note: Data refer to 2010 and are estimates
Source: ITU World Telecommunication/ICT Indicators database

ICT diffusion
Mobile Broadband



ICT diffusion
Mobile Broadband

Evolution Path of 2G and 3G Technologies

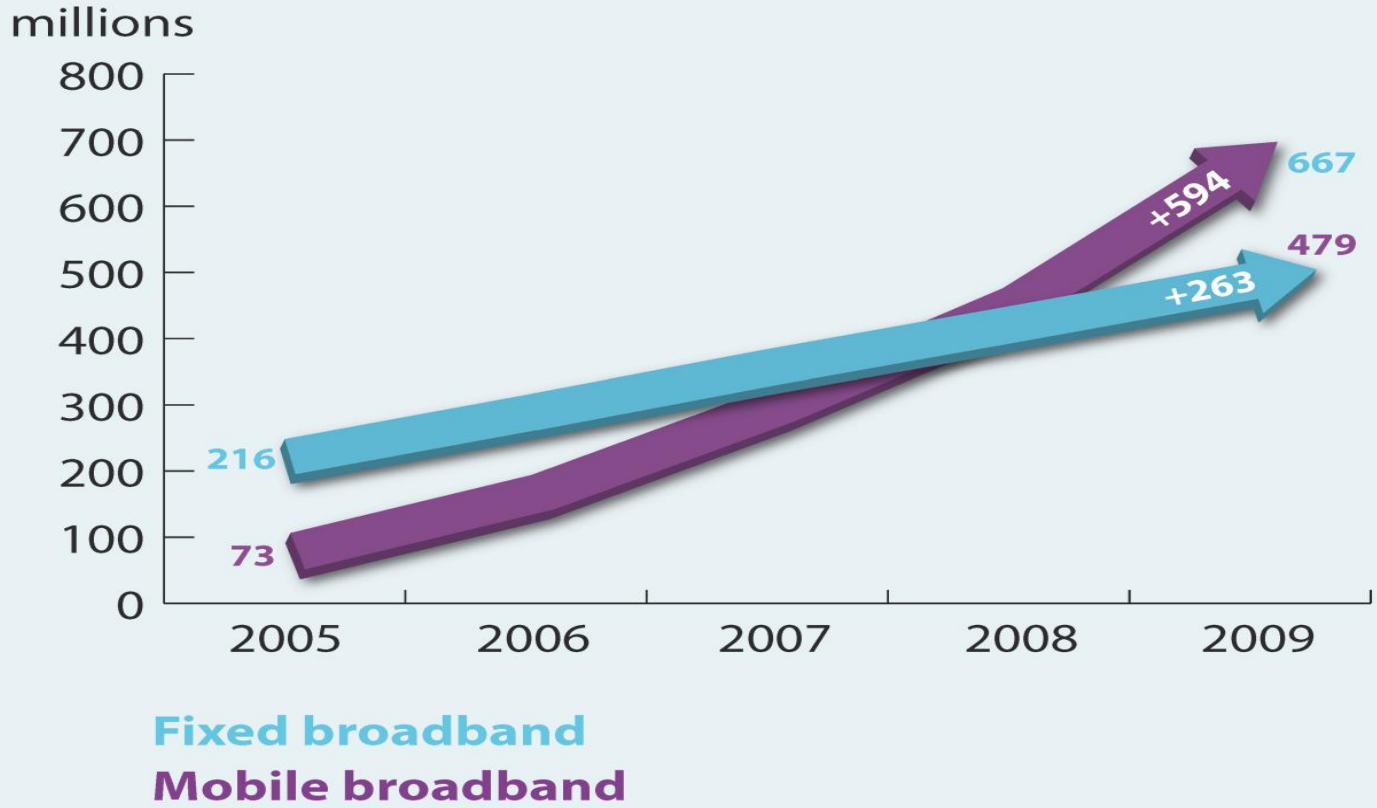


Source: Wireless Intelligence, April, 2009

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

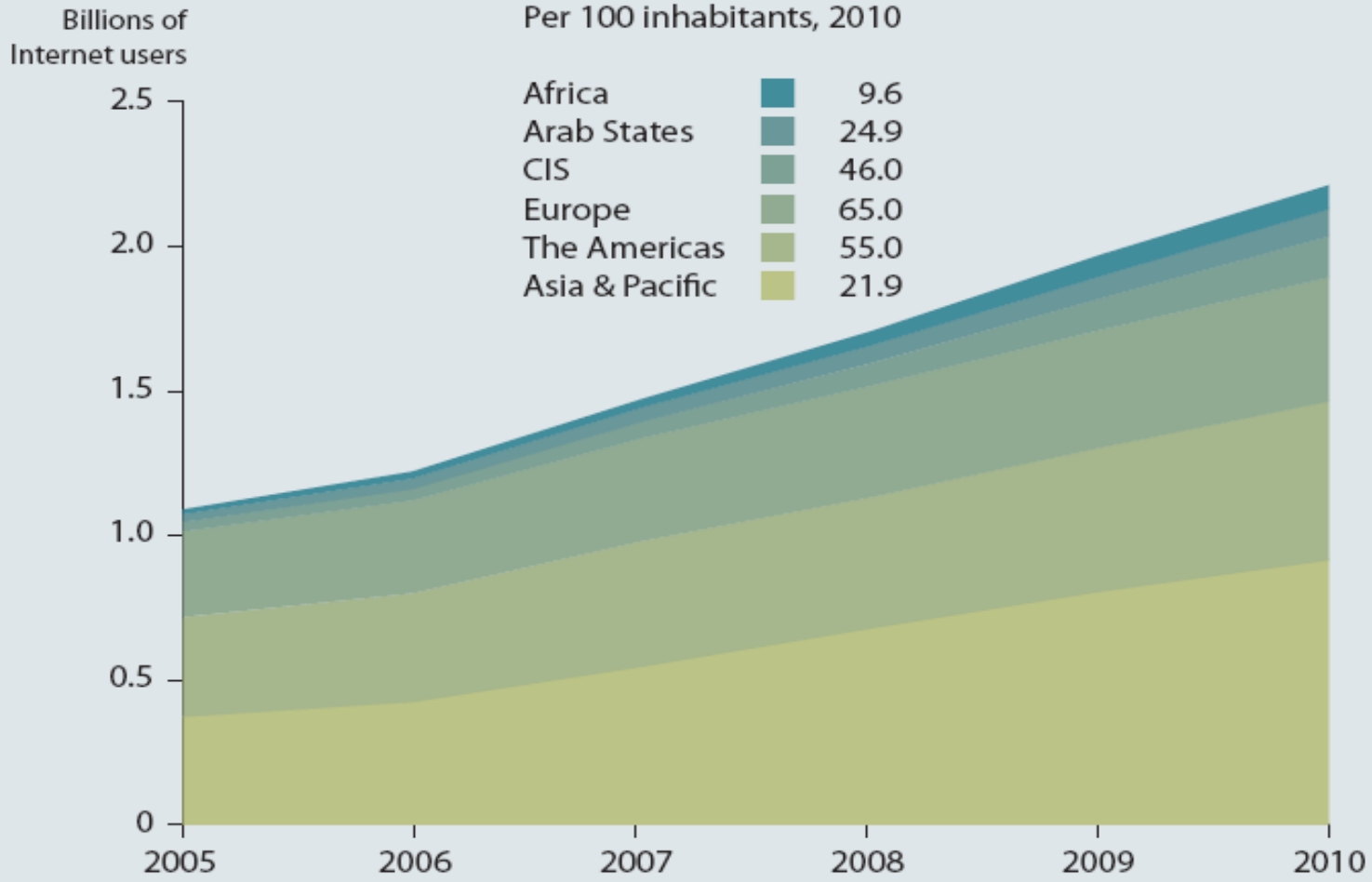
ICT diffusion
Broadband

Broadband subscriptions, 2005-2009



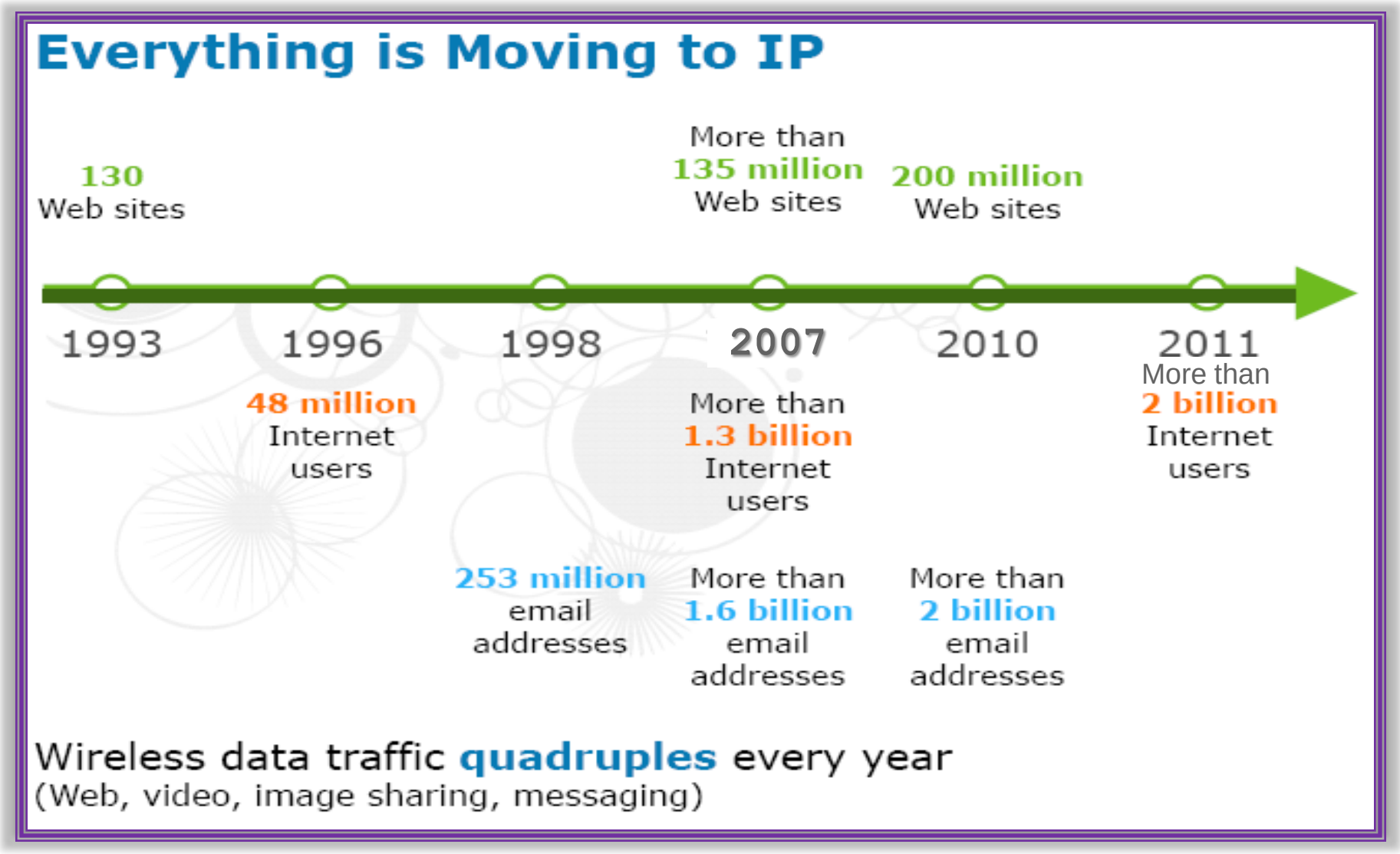
Source: ITU

ICT diffusion
Internet



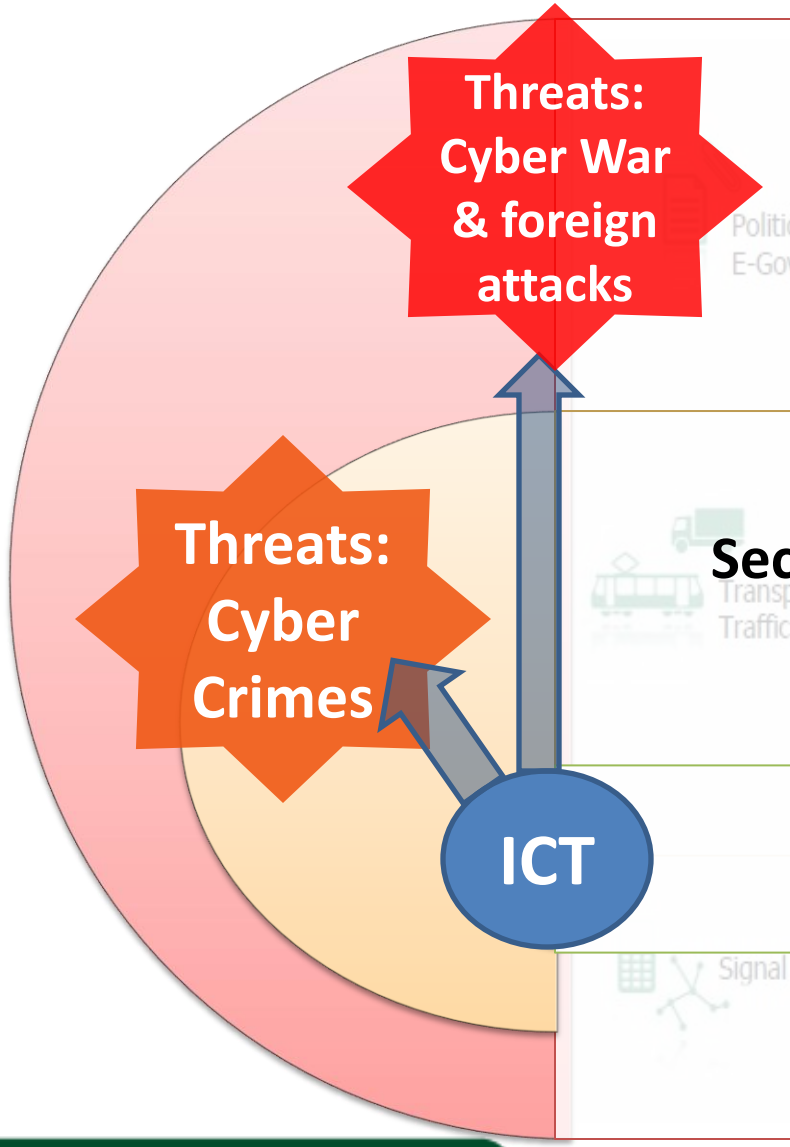
*Note: *Estimate*
Source: ITU World Telecommunication/ICT Indicators database

ICT diffusion
Internet



ICT & threats - Secondary effects –

ICT & Threats



Public & Basic services

- **Civil:** Energy, Communications, Water supply & drainage, transportations, etc…
- **Military:** Command & Control, Intelligence, defense, etc…
- **Internal security**: Investigation & Forensics, Emergency, etc…

Sector Specific

- **Economy & business**: Industry, Banking, E-commerce, agriculture, etc…
- **Education**: E-learning, E-libraries, etc…
- **Health**: Tele-health, assisted Surgery, etc…
- **Social**: Global literacy, capacity building, rights to access information (Personal information & Children online issues), etc…

- **Fixed & Mobile Infrastructures**
- **Internet Capacity & access**
- **Computers & IT applications & Media & RTTEs**

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

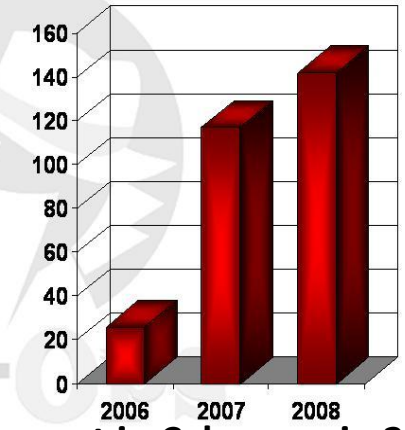
INTELLIGENCE BRIEFING

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.

Countries with cyber weapons programs

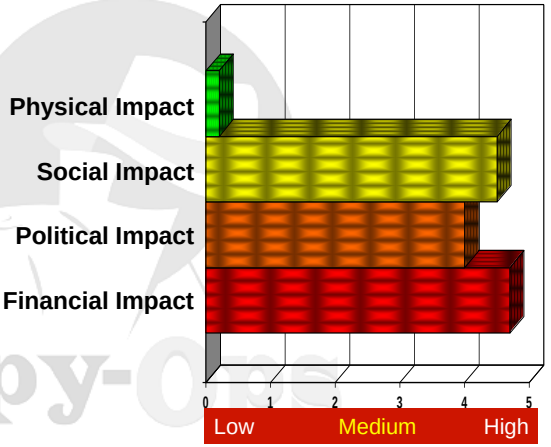


INTELLIGENCE BRIEFING

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!

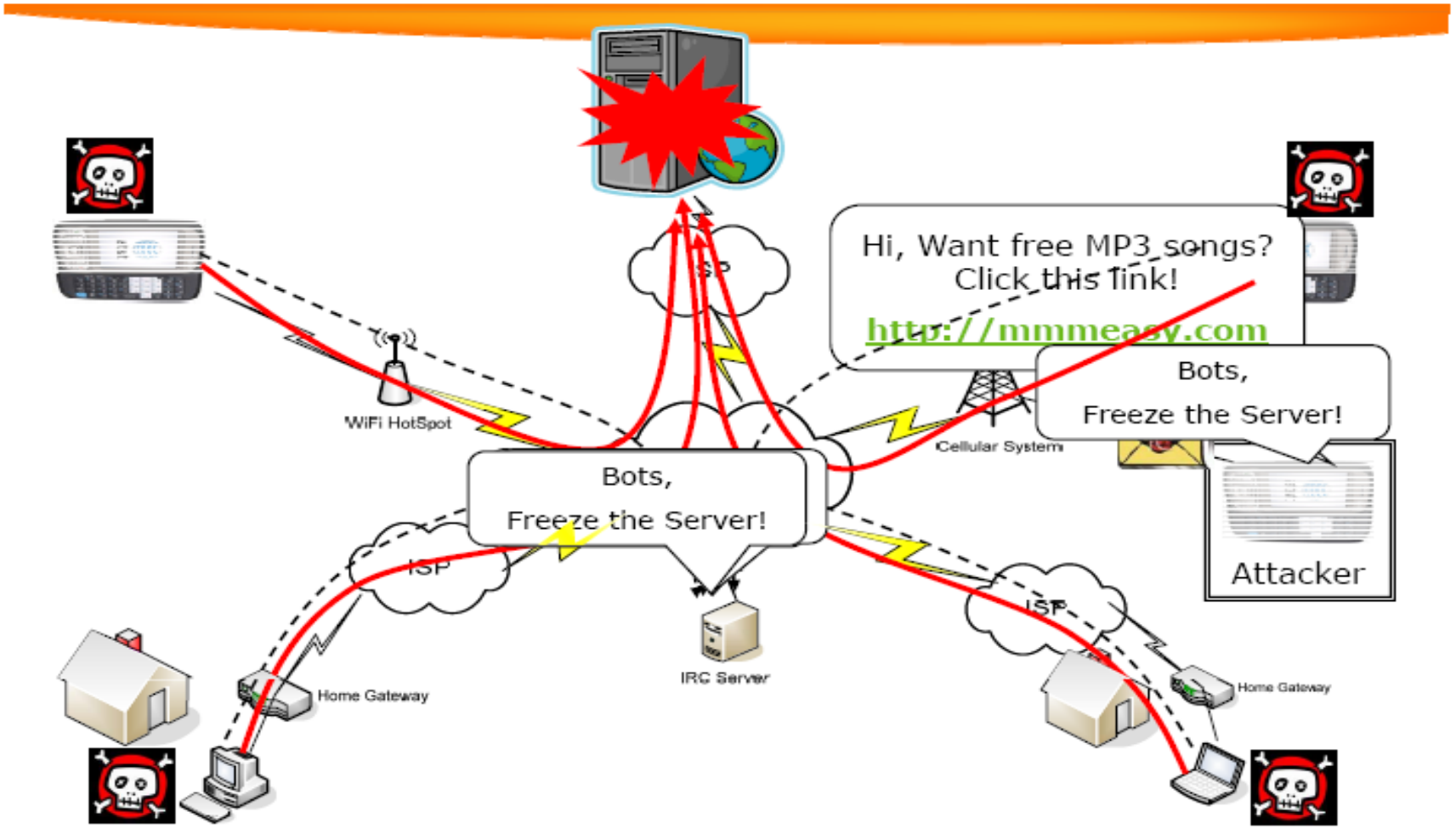


www.Spy-Ops.com

2

- **Government involvement in Cyberwar in 2009**
  - **April:** The UK government confirms plans for a £2 billion tracking system to snoop network traffic for 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, media has revealed the existence of the unit 8200 within the Israeli intelligence dedicated for Cyber war and attacks.

ICT & Threats
Cyber Crimes

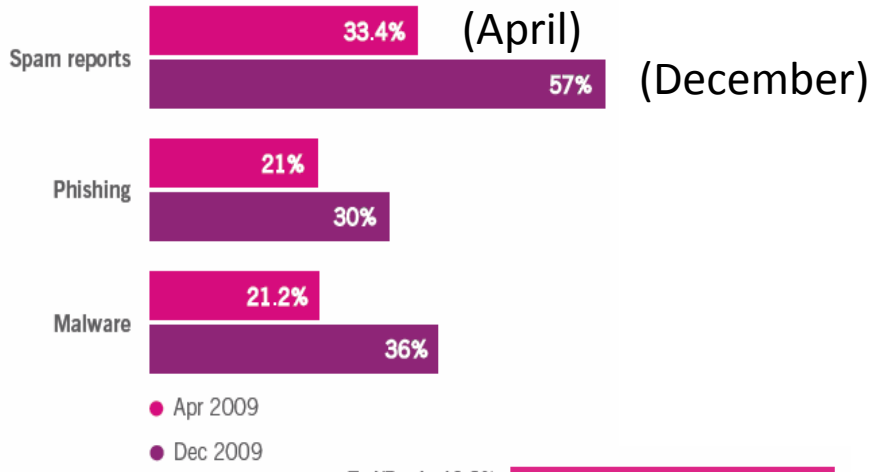


Threats Associated with Living With ICTs
Cyber Crimes

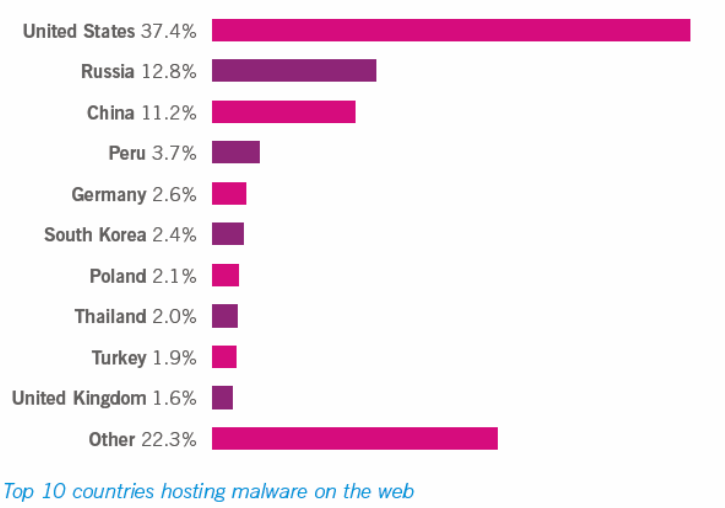
- Hacking
- Pirated Software & CDs
- Pornography
- Bad Films & Sites that Affect Ethics and Children
- Sale of Illegal Items & Personal Information
- Preying On Children
- Intelligence/ Military Attacks
- Spread of Virus/ Malware
- Racism & Violence
- Terrorism
- Fencing Stolen Goods
- Online Gambling & Addiction
- Online Fraud
- Identity Theft

Threats Associated with Living With ICTs
Cyber Crimes (Sophos security report -2010)

- Social networks threats

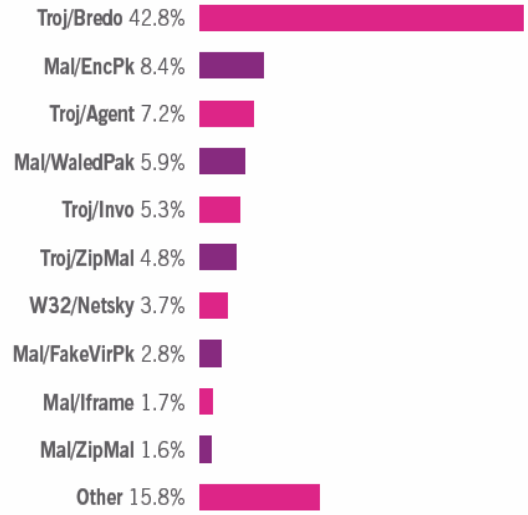


- Web threats



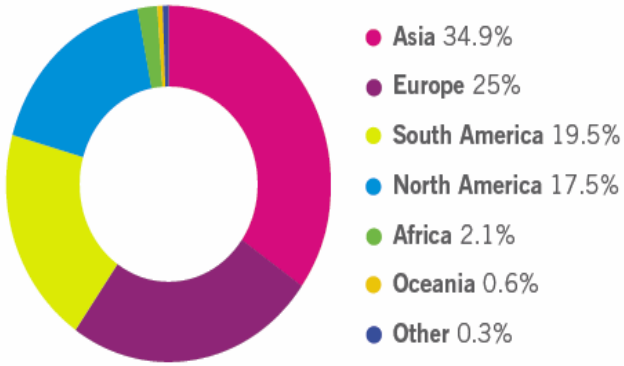
Top 10 countries hosting malware on the web

- E-mail threats



Top 10 malware spreading via email in 2009

- Spam



Spam by continent

Teens & ICT– Vulnerability, Threats and Measures

Teens & ICT
Social and Legal general environment

- Around 90% of teens and young adults use the Internet
- Over 60% of children and teenagers talk in chat rooms on a daily basis.
- 3 in 4 children online are willing to share personal information about themselves and their family in exchange for goods and services
- 1 in 5 children will be targeted by a predator or pedophile each year
- While 30% of teenage girls say they have been sexually harassed in a chat room, only 7% tell their parents (for fear their online access will be limited.)

Risks to Children Online

CONTACT

- Unwanted Contact
- Cyberbullying
- Child Predators

CONTENT

- Inaccurate Content
- Extreme Views / Hate Speech
- Questionable Material
- Online Reputation

COMMERCE

- Product / Service Solicitations
- Privacy Issues / Identity Theft

Teens & ICT Threats

Threats identification (ITU guide, 2009)

Films and Sites that affect ethics and personality

Online Fraud

Child pornography

Online Gaming & Addiction

Violence

Illegal Gambling

Insults and Labeling

Identity Theft

Cyber-bullying

Racism

Teens & ICT Facts

Facts from around the Globe (ITU statistics, 2009)

- In France, 72% of children surf online alone, and while 85% of parents know about parental control software, only 30% have installed it
- In Korea, 90% of homes connect to cheap, high-speed broadband, and up to 30% of Koreans under the age of 18 are at risk of Internet addiction, spending two hours a day or more online
- In the UK, 57% of 9-19 year olds say they've seen online pornography, 46% say they've given out information they shouldn't and 33% say they've been bullied online
- In China, 44% of children said they had been approached online by strangers, and 41% had talked to an online stranger about sex, or something that made them feel uncomfortable

Children when accessing the internet could be targets of pedophiles, cyber bandits, hackers and online predators.

ICT & Youth
Child Pornography

Threats identification (ITU guide, 2009)

- In contrast to differing views on adult pornography, child pornography is broadly condemned and offences related to child pornography are widely recognized as criminal acts
- International organizations are engaged in the fight against online child pornography, with several international legal initiatives including:
  - the 1989 United Nations Convention on the Rights of the Child
  - the 2003 European Union Council Framework
  - Decision on combating the sexual exploitation of children and child pornography; and
  - the 2007 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse

- Research into the behavior of child pornography offenders shows that
  - 15 % of arrested child pornography offenders had more than 1,000 pictures on their computer;
  - 80 %had pictures of children between 6-12 years on their computer;
  - 19% had pictures of children younger than the age of 6;
  - 21% had pictures depicting violence.

Child online protection Solution?

- COP aims to tackle Cybersecurity holistically, addressing legal, technical, organizational and procedural issues as well as capacity building and international cooperation
- **There is no one technological solution or specific combination of technological solutions** to the problem, but a combination of:
  - Technologies
    - Parental Oversight
      - Education
        - Social Services
          - Legal and Regulatory Framework and Law Enforcement
            - Sound Policies by Social Network Sites and Service Providers
- All stakeholders must continue to work in a cooperative and collaborative manner, sharing information and ideas to achieve the common goal of making the Internet as safe as possible for minors

Child online protection
Solution?...some considerations

- Some technical protection measures
  a) Age verification, Identity Authentication, and Biometrics
  b) Filtering, Auditing and Text Analysis
- Technologies presents **privacy and security issues** that must be weighed against potential benefits
- May carry an economic cost and require involvement by parents and teachers
- Relying on technologies may not protect most vulnerable minors
- Steps by the social network sites are helpful in mitigating some risks, but none is fail-safe
- The development of technologies can play a helpful role in enhancing protections of minors
- Supporting institutions and individuals working on the net are effective participants in the protection of minors

ICT & Youth
Best practices and policies

ITU Recommendations (April , 2009)

- **Create Public awareness** in matters concerning the protection of children in Cyberspace, with a clear definition of policies, best practices, tools and necessary resources needed to adapt and use in each country
  - Children and young people online should be aware of the opportunities as well as the pitfalls
- **Support efforts** aimed at developing guidelines on the online child protection by policy makers and regulators
- **Identify risks and vulnerabilities** faced by children in cyberspace as ICT technologies (Internet and other electronic resources) are in permanent ongoing expansion
- **Build dedicated containers** of resources for shared use
- **Promote capacity-building** aimed to strengthening the global response to protect children during their adventures in cyberspace

ICT & Youth
Best practices and policies

The EUROPEAN PARLIAMENT AND COUNCIL therefore recommends to:

1. Take actions to enable minors to make responsible use of audiovisual and on-line information services by improving the level of awareness among parents, teachers and trainers
2. Draw-up a code of conduct in cooperation with professionals and regulatory authorities at national and Community level
3. Adopt a quality label for service providers, so that users can easily check whether or not a given provider subscribes to a code of conduct
4. Examine the possibility of creating filters which would prevent information offending against human dignity from passing through the Internet
5. Develop measures to increase the use of content labeling systems for material distributed over the Internet
6. Explore the possibility of supporting the establishment of a generic second level domain name reserved for monitored sites committed to respecting minors and their rights, such as .KID.eu

Child online protection
Developed world

- **In developed countries, some of the measures that have being taken**
  - In Germany, the Youth Protection Act 2003 requires companies who wish to provide content that is not suitable for minors to offer a youth protection scheme. These schemes have to be validated by a new official body. The act makes no distinction between mobile and fixed internet services
  - Britain's mobile operators have announced a new Code of Practice designed to prevent underage and unauthorized users from accessing pornographic images and other adult content and services on their mobile phone
  - The EU is holding an exploratory meeting called "Towards a European Code of Conduct for ISPs" focused on the issue of illegal & harmful Internet content
  - In Japan, new laws promoting self-regulation address child protection issues, especially in relation to mobile dating services. Public funds are available for education campaigns and for developing improved filtering technologies

Child online protection
Vision of a National Child Online Protection Strategy

Based on international best practices and recommendations

There is a need to set up the Cyberspace Protection Center for Lebanon, which is a jointly Private-Public Administration (PPA) having a dedicated section for online children and youth protection. Other recommendations include:

- **To develop a national strategy to promote the safe use** of ICT, and the dissemination of such "guided" use on all layers of Lebanese society
- **To develop a national strategy to identify all sources of threats and risks** that might face children, not only through the Internet, but that also include all ICT Medias
- **The Establishment of a permanent national cooperation framework** between the government, the public sector, and the private sector to continuously update the protective measures and meet the challenges arising from the ongoing technological advances
- **Making recommendations to the government** for the enactment of necessary legislation and measures
- **Promoting a culture of awareness** that widely explains the foundations of Cybersecurity that are related to risks facing children and minors using any of the communication and information technology means and tools
- **Coordinating and cooperating with other regional and international organizations**, and following up with equipment manufacturers and major ICT solution providers, holding all necessary peer to peer agreements and memos that help deploy appropriate solutions in Lebanon
- **Adopting the recommendations of the European Parliament & ITU** and inspire the models in place by the European countries and developing national policies and ways of application
- **Taking into account in all future legislations children online protection**

Child online protection
Lebanese efforts

Children online protection - Current Efforts

- The Higher Council for Children Protection in the Ministry of Social Affairs
  - **Technical committee**
    - ✓ **develops recommendations on technical solutions (although no final recommendations have been issued yet)**
  - **Media committee**

    In charge of:
    - ✓ **awareness campaigns**
    - ✓ **guidance and direction for parents and educational institutions**
    - ✓ **social developments that focus on online risks that children face and the best ways to address them**
  - **Legal Committee**
    - ✓ **converts suggestions/recommendations on threats facing children online to the binding legal texts of laws, decrees and other legal/administrative means**
- Internet Service Providers (ISP's)
  - **Some ISP's have dedicated Parental Control systems that are promoted on their WebPages (at Symbolic fees or free of charge)**
  - **Others give tips and hints for parents about buying and downloading children protection tools**

Rate of subscribers using parental control tools is only 0.7%! of the overall internet subscribers at Ogero

Child online protection
Possible regulatory measures to be undertaken by the TRA

The TRA, in cooperation with law enforcement agencies and municipalities may ask owners of Internet cafes to

- **Abide by enforced laws**
  - **Securing protected areas designated for the use of children and minors**
  - ✓ **age verification**
  - ✓ **identity check**
  - ✓ **content filtering and text analysis**
  - ✓ **Checking contents to be used by children**
- **Maintain stored data and traffic** data information and log use in a safe place for a "specific" period of time
- **Provide direct access and necessary facilities "to those legally entitled to" personnel** (having permission according to proper judicial process)
- **Ensure that personal data is**
  - ✓ Appropriate, useful and not excessive and collected and used for the informative use only
  - ✓ Accurate and updated when needed and is retained only for the period for which it was collected
  - ✓ Addressed according to the legal manner and treated in accordance with personnel data rights
- **Take all measures to protect against unauthorized access** such as manipulation / loss of personnel data
- **Protect the privacy of personal information** collected from monitoring the use of children
- **Write a contractual obligation** in which they comply to applied rules related to dealing with data and ensure that above arrangements exist and are in place

Cybersecurity – Urgent needs for a solution

Steps Towards Developing a Culture of Cyber Security

- Strategies for the development of a global framework for security protocols, standards, software and hardware accreditation schemes
- Review existing privacy regime and update it to the online environment

- Elaboration of global strategies for the creation of appropriate national and regional organizational structures and policies
- Cooperation between all institutions

- Create awareness at a national policy level
- Harmonization of legal frameworks
- Develop cooperative relationships with other elements of the national cyber security infrastructure and the private sector

- Development of proposals to enhance international dialogue on issues that pertain to cyber security and enhance cooperation and coordination
- Participate in international efforts to promote national prevention of, preparation for, response to, and recovery from incidents

- Increased public awareness and education
- Development of global strategies to facilitate human and institutional capacity building
- Training for criminal justice professionals
- Encourage the private sector to report any information they might obtain concerning cybercrime to the appropriate law enforcement or social service authority

Steps Towards Developing a Culture of Cyber Security (1/2)

❑ **Legal Measures:**

- Create awareness at a national policy level (including policy makers) about cyber security issues and the need for national action and international cooperation
- Harmonization of legal frameworks and the elaboration of strategies for the development of cybercrime legislation that is globally applicable and interoperable with existing National legislative measures
- Develop cooperative relationships with other elements of the national cyber security infrastructure and the private sector
- Develop an understanding among prosecutors, judges, and legislators of cybercrime issues

❑ **Technical and Procedural Measures:**

- Strategies for the development of a global framework for security protocols, standards, software and hardware accreditation schemes
- Review existing privacy regime and update it to the online environment

❑ **Organizational Structures:**

- Elaboration of global strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime watch, warning & incident response
- Cooperation between all institutions (at national and international level) and law enforcement agencies in fighting against cybercrime

Steps Towards Developing a Culture of Cyber Security (2/2)

- **Capacity building:**
  - Development of global strategies to facilitate human and institutional capacity building across all relevant aspects of cyber security
  - Increased public awareness and education about the danger of the computer crimes
  - Encourage the private sector (including Internet Service Providers) and civil society (including teachers, non-governmental organizations, the media) to report any information they might obtain concerning cybercrime to the appropriate law enforcement or social service authority
  - Training for criminal justice professionals (law enforcement, prosecutors and the judges) is a necessary as a part of a comprehensive program designed to fight these crimes
  - Promote a national culture of cyber security: support outreach to civil society with special attention to the needs of children and individual users

- **International cooperation:**
  - Development of proposals to enhance international dialogue on issues that pertain to cyber security and enhance cooperation and coordination across all relevant activities
  - Participate in international efforts to promote national prevention of, preparation for, response to, and recovery from incidents

Cyber Security: Roles and Responsibilities

The Government

- Policy-making as well as ensuring that the national policy is flexible and adaptive
- Legal Measures: creating new (or adapting existing) legislation to curb abuses and protect consumer rights
- Organizational Structures:
  - Institutional organization and coordination
  - Incident management and cyber security readiness assessment
- Capacity Building
- Public-private sector cooperation and industry regulation

The Private Sector

- Implementing an adequate level of cyber security safeguards in their business practices:
  - the installation of technical solutions
  - the adoption of secure business processes
- Cooperating with government in:
  - developing cyber security business norms, standards and codes of conduct
  - identifying and encouraging the adoption of good practices
- Agreeing on technical standards to protect security by taking part in relevant forums or standards-development organizations

The Individual

- Getting familiar with cyber security threats (e.g. viruses, spam, etc.)
- Adopting the appropriate technical safeguards (e.g. anti-virus software, firewalls, etc.)

The Civil Society

- Understand the range of societal issues cyber security raises
- Provide feedback and other contributions that can serve as an important source for policy-makers that seek to create a cyber security approach, in consultation with the government


THANK YOU