Cyber Security Organizations and Efforts

Dr. Imad Y. Hoballah
Commissioner, Board Member
Head of Telecommunications Technologies Unit
Telecommunications Regulatory Authority (TRA), Lebanon

Agenda

- ❑ Cyber Security: Definition, Threats, Roles & Responsibilities
- ❑ International Intergovernmental Organizations
- ❑ Regional Intergovernmental Organizations
- ❑ Private-Public & Non-Governmental Organizations
- ❑ Selected Country-Specific Organizations
- ❑ Arab Organizations
- ❑ Pan Arab Observatory for Cybersecurity

Cyber Security: Definition, Threats, Roles & Responsibilities

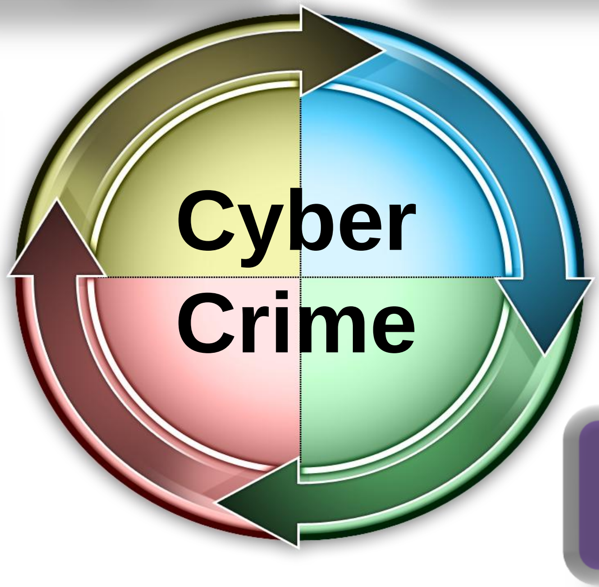
Cyber Security Definition

- ❑ It is the set of:
  - Regulatory frameworks
  - Working procedures
  - Technical and Technological means

    that are used for the prevention of unauthorized use, exploitation of, and the restoration of electronic information and communications systems, and the information they contain

- ❑ With emphasis on
  - Availability of the information systems
  - Strengthen the confidentiality and protect privacy of personal data
  - All necessary measures to protect Citizens and Consumers against risks in Cyberspace

Threats Associated with Living With ICTs: Cyber Crimes

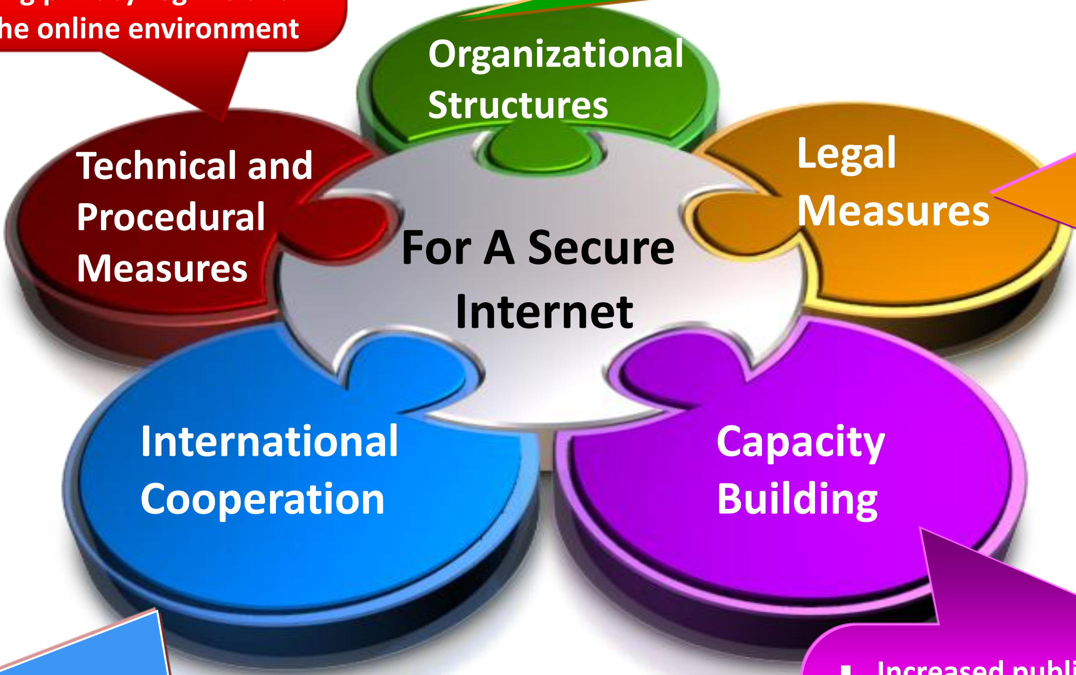


- Hacking
- Pirated Software & CDs
- Pornography
- Bad Films & Sites that Affect Ethics and Children
- Preying On Children
- Sale of Illegal Items & Personal Information
- Intelligence/ Military Attacks
- Spread of Virus/ Malware
- Racism & Violence
- Terrorism
- Fencing Stolen Goods
- Online Gambling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

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


Organizational Structures
Technical and Procedural Measures
For A Secure Internet
Legal Measures
International Cooperation
Capacity Building

- 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

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

International Intergovernmental Organizations

International Intergovernmental Organizations

- United Nations (UN)
  - International Telecommunication Union (ITU)
    - ITU Corporate Strategy Division (CSD)
    - ITU Radio communication Sector (ITU-R)
    - ITU Telecommunication Development Sector (ITU-D)
    - ITU Telecommunication Standardization Sector (ITU-T)
    - World Trust Signatories Association (WTSA)
    - WSIS Thematic Meeting on Countering Spam
  - United Nations Office for Disarmament Affairs (UNODA)
  - United Nations Office on Drugs and Crime (UNODC)
- World Customs Organization (WCO)
- Organization for Economic Co-operation and Development (OECD)
- Group of Eight (G8)
  - G8 24/7 Network of Contacts for High-Tech Crime
- International Law Enforcement Telecommunications Seminar (ILETS)
- International Criminal Police Organization (INTERPOL)
- North Atlantic Treaty Organization (NATO)

International Intergovernmental Organizations

❑ **United Nations Office on Drugs and Crime (UNODC)**

- Established to help the UN address the interrelated issues of illicit-drug control, crime prevention, and international terrorism.
  - through three primary functions: **research, lobbying** state governments to adopt various crime and drug based laws and treaties, and **assistance** of said governments on the ground level
- UNODC initiatives include the promotion of cybercrime legislation, law enforcement, and training programs

❑ **World Customs Organization (WCO)**

- The only worldwide intergovernmental organization focused exclusively on customs matters. Due to its role in facilitating global supply chain security, the WCO has taken an active role in promoting strategies on Critical Infrastructure Protection (CIP) and electronic crime
- **Focuses on defense of electronic infrastructures, early warning of potential vulnerabilities, countering threats to core ICT** competencies, keeping pace with new technologies, and providing recommendations for training and technological development

❑ **Group of Eight (G8):**

- An international forum for the governments of Canada, France, Germany, Italy, Japan, Russia, UK, and the US
- An attempt to provide information sharing mechanisms among major industrialized powers & enhance the abilities of G8 countries to **prevent, investigate, and prosecute crimes** involving computers, networked communications, and other new technologies

❑ **International Law Enforcement Telecommunications Seminar (ILETS)**

- Initiated by the US Federal Bureau of Investigation (FBI) in 1993
- Is an annual gathering of law enforcement and national security agencies from a number of countries for cooperation on lawful telecommunications interception and data retention
- The founding members are Australia, Canada, Hong Kong, US, and UK
  - plus Norway, Denmark, France, Germany, Netherlands, Spain, and Sweden

❑ **International Criminal Police Organization (INTERPOL)**

- The world's largest international police organization with 186 member countries
- Facilitates cross-border police cooperation, and supports and assists all organizations, authorities, and services whose **mission is to prevent or combat international crime**
- Based in Europe, INTERPOL limits its involvement to crimes that occur in more than one member country.
- **ICT crime, in particular, is handled as a sub-directorate under Financial and High Tech Crime**

International Intergovernmental Organizations

- ❑ **International Telecommunication Union (ITU)**
  - The only intergovernmental organization within the UN system that has partnerships between government and industry
  - Involved in building confidence and security in the use of ICTs, facilitating cooperation among public/private organizations, and fostering education and training initiatives

- ❑ **ITU Corporate Strategy Division (CSD)**
  - Works to identify trends in the evolution of cyber security, spam, and cybercrime, and establishes corporate strategy objectives for the ITU
  - Also maintains an updated website page regarding cyber security-related activities of the ITU Corporate Strategy, called the Cybersecurity Watch News log.

- ❑ **World Trust Signatories Association (WTSA)**
  - Established by ITU-D in 2002 to facilitate a highly secure ICT infrastructure for developing countries
  - Projects: Partnering with Quiet Enjoyment Infrastructure (QEI), in March 2005 the ITU introduced the City of Osmio, an online-only municipality, as an experiment to demonstrate authenticity over the World Wide Web using trusted public key infrastructure and digital certificates

- ❑ **ITU Radiocommunication Sector (ITU-R)**
  - The primary contribution of ITU-R to the global cyber security initiative - includes references to security in its numerous ITU-R recommendations
  - Recommendations particularly relevant to cyber security include Recommendation 1078: Security principles for IMT-2000 and Recommendation 1223: Evaluation of security mechanisms for IMT-2000. Security mechanisms in IMT-2000 are also referenced in Recommendation 1457, and references to security in other systems can be found in Recommendations M.1645 and M.2063

- ❑ **ITU Telecommunication Development Sector (ITU-D)**
  - The ICT Applications and Cybersecurity Division (CYB) is the ITU Telecommunication Development Sector's (ITU-D) focal point to assist developing countries through the use of information and communications technologies (ICTs) and telecommunications networks, to advance the achievement of national, regional and the internationally agreed development goals, by promoting the use of ICT-based products, networks, services and applications, and to help countries overcome the digital divide

International Intergovernmental Organizations

❑ **ITU Télécommunications Standardization Sector (ITU-T)**

- The World Telecommunication Standardization Assembly (WTSA), which supports the implementation of general policy mechanisms and working methods for ITU-T, deliberated on several key issues pertinent to cyber security, such as next generation networks (NGN), bridging the standardization gap between developing and developed countries, consensual decision-making, new resolutions on Internet-related issues, and the adoption of a resolution on cyber security
- ITU-T has also hosted numerous other workshops and conferences to effect cyber security standards in the information society
- ITU-T Study Group 17, the lead telecommunication security group, has been especially active in promoting cyber security initiatives, providing numerous forums and focus groups in which topics on security guidance, identity management, and security standards may be presented

❑ **WSIS Thematic Meeting on Countering Spam**

- Following the WSIS Thematic Meeting on Countering Spam, the ITU launched a comprehensive online database devoted to all spam-related issues, including background resources, documentation, presentations, contributions, and technical papers on the issues presented at the event, including spam legislation and enforcement, technical solutions, international cooperation, and consumer education and awareness
- Additionally, the ITU provides detailed information on upcoming spam-related conferences and events hosted by partners in the international community, such as StopSpamAlliance.org

❑ **North Atlantic Treaty Organization (NATO)**

- Is an alliance of twenty-six countries from North America and Europe that provides an international forum for the discussion of common security issues

❑ **Organization for Economic Co-operation and Development (OECD)**

- Is an international forum bringing together the governments of thirty member countries, as of 2008, committed to democracy and market economies
- Provides a **setting where governments compare policy experiences,** seek answers to common problems, identify good practices, and coordinate domestic and international policies

Regional Intergovernmental Organizations

Regional Intergovernmental Organizations

- ❑ **Americas**
  - ➢ Latin American Cooperation of Advanced Networks (CLARA)
    - ❖ CLARA Computer Security Incident Response Team (GT-CSIRT)
    - ❖ CLARA Security Task Force (GT-Seg)
  - ➢ Organization of American States (OAS)
    - ❖ Group of Governmental Experts on Cyber-Crime
    - ❖ Inter-American Committee Against Terrorism (CICTE)
    - ❖ Inter-American Telecommunication Commission (CITEL)
- ❑ **Asia-Pacific**
  - ➢ United Nations Economic and Social Commission for Asia and the Pacific (ESCAP)
  - ➢ Asia-Pacific Economic Cooperation (APEC)
  - ➢ Asia Pacific Computer Emergency Response Team (APCERT)
  - ➢ Asia-Pacific Telecommunity (APT)
  - ➢ Association of Southeast Asian Nations (ASEAN)
    - ❖ ASEAN Regional Forum (ARF)
    - ❖ ASEAN Telecommunications and IT Ministers (TELMIN)
  - ➢ China-Japan-Korea (CJK)

- ❑ **Europe**
  - ➢ European Committee for Standardization (CEN)
  - ➢ Council of Europe (COE)
  - ➢ European Network and Information Security Agency (ENISA)
  - ➢ European Telecommunications Standards Institute (ETSI)
  - ➢ European Union (EU)
    - ❖ European Law Enforcement Organisation (Europol)
    - ❖ European Union Contact Network of Spam Authorities (CNSA)
  - ➢ ICT Standards Board (ICTSB)
  - ➢ National Policing Improvement Agency (NPIA)
  - ➢ Organization for Security and Co-operation in Europe (OSCE)
  - ➢ Trans-European Research and Education Networking Association (TERENA)
    - ❖ European Task Force on Computer Security Incident Response Teams (TF-CSIRT)

Regional Intergovernmental Organizations - *Americas*

❑ **Latin American Cooperation of Advanced Networks (CLARA)**

- A nonprofit, regional intergovernmental organization created in November of 2004 to provide connectivity to the Americas and link national research and education networks within Latin America and with other networks in Europe (GEANT2), the United States (Internet2), Asia (APAN) and the rest of the world
- Since its creation, CLARA has established a platform that links 12 countries and 729 universities throughout the Americas at speeds of up to 622Mbps

➢ **CLARA Computer Security Incident Response Team (GT-CSIRT)**

- ○ Promotes incident response initiatives in the Americas
- ○ Its work includes: **proposals** for defining security profile roles for each Member State, **requesting directive support** to define security contacts, **promoting the establishment of new CSIRTs** in the region using a Security Training and Education Program (STEP), **building a security best practices** digital repository, **organizing regular meetings and seminars** as part of the Security Awareness Program (SAP), **collaborating with other CLARA** Task Forces and Working Groups, and promoting **collaborative activities** among regional and international CSIRTs

➢ **CLARA Security Task Force (GT-Seg)**

- ○ Is a Security Task Force (GT-Seg) created by CLARA based on CSIRTs participation to promote a security culture in the Latin American and Caribbean region
- ○ GT-Seg is committed to establishing computer security frameworks in each member state, promoting the development of new CSIRTs in the region, providing a discussion forum for information sharing, facilitating exchange and data correlation of security incidents, promoting a coordinated response to security incidents, disseminating security best practices for academic environments, building an updated database of security points-of-contact for each member state, and cooperating with other regional initiatives

Regional Intergovernmental Organizations - *Americas*

- ❑ **Organization of American States (OAS)**
  - Represents the largest regional cooperation effort within the Americas
  - Formed in 1948 by the Ministers of Justice or Ministers or Attorneys General of the Americas (REMJA), OAS is composed by thirty-five member states from the Western Hemisphere, and the organization is primarily concerned with interaction and cooperation among its member states
  - ➢ **Group of Governmental Experts on Cyber-Crime**
    - Has a mandate to perform the following actions: complete a **diagnosis of criminal activities** that target computers and information or that uses computers as the means of committing an offense; complete a **diagnosis of national legislation, policies, and practices** regarding such activity; identify **national and international entities with relevant expertise**; and identify **mechanisms of cooperation** within the Inter-American system to combat cybercrime
  - ➢ **Inter-American Committee Against Terrorism (CICTE)**
    - Addresses **cyber security through work on incident response** in the Americas region and holds frequent meetings, workshops, and conferences on cyber security throughout the Americas that emphasize CIIP, cyber terrorism, and incident response
  - ➢ **Inter-American Telecommunication Commission (CITEL)**
    - Is an entity of the Organization of American States whose objective is to facilitate and promote the continuous development of telecommunications in the Hemisphere
    - CITEL has a working group specifically tasked with cyber security and critical infrastructure protection
    - CITEL also holds regional workshops several times a year on combating fraud in telecommunication services, promoting information exchange, research, and discussion on legislation, regulation and control, technical and administrative tools, and inter-State and inter-sectorial mutual cooperation mechanisms to minimize the effects of fraud

Regional Intergovernmental Organizations – *Asia-Pacific*

❑ **United Nations Economic and Social Commission for Asia and the Pacific (ESCAP)**

- The regional development arm of the United Nations for the Asia-Pacific region
- ESCAP has hosted numerous workshops, seminars, and symposiums on ICT capacity building and enabling policies and regulatory frameworks for ICT development in the Asia-Pacific region
- ESAP has also released major publications related to ICT policy

❑ **Asia-Pacific Economic Cooperation (APEC)**

- The primary organization responsible for facilitating economic growth, cooperation, trade, and investment in the Asia-Pacific region
- Issued APEC's Cyber-Security Strategy which identified six areas that serve as the basis for APEC's efforts on cybercrime and critical infrastructure protection
- Holds semi-annual meetings to discuss the status of cyber security in the Asia-Pacific region
- Currently working with the APEC Counter Terrorism Task Force (CTTF) on issues related to cyber terrorism
- Also working with the private sector to identify new technologies and challenges related to Next Generation Networks (NGN)

❑ **Asia Pacific Computer Emergency Response Team (APCERT)**

- Handles incident response coordination efforts and enables regional cooperation in the Asia-Pacific rim
- Holds Annual General Meetings to provide an opportunity for APCERT members to meet and learn about issues affecting each other as CERTs
- Holds an annual drill to test the timeliness and response capability in addressing regional cyber threats of leading CSIRTs from Asia-Pacific economies

❑ **Asia-Pacific Telecommunity (APT)**

- Promote the explanation of telecommunication services and information infrastructure , and facilitates coordination within the region with regard to major issues pertaining to telecommunication services. APT has only started to play a role in the cyber security arena in the past few years, with an apparent focus on issues related to spam
- Organized seminars on "CERT Best Practices" and held a sub-regional Meetings on Spam and Security, and on Network Security

Regional Intergovernmental Organizations – *Asia-Pacific*

❑ **Association of Southeast Asian Nations (ASEAN)**

- Accelerates economic growth, social progress, and cultural development in the region and promotes regional peace and stability through abiding respect for justice and the rule of law in the relationship among countries in the region
  - **Asia-Pacific Telecommunity (APT)**
    - Organizes an annual Seminar on Cyber Terrorism.
    - Previous seminars have focused on such topics as assessing the implications of cyber terrorism on national and global security, private-government partnerships, creation of CSIRTs, harmonization of domestic laws and regulations, and the enhancement of cooperation amongst members
    - Created a Virtual Working Group (VWG) on Cyber Security and Cyber Terrorism
  - **ASEAN Telecommunications and IT Ministers (TELMIN)**
    - Focuses mainly on building capacity and cooperation relating to ICT
    - Current activities include establishing a national Computer Emergency Response Team (CERT), establishing guidelines for information sharing among CERTs, developing a convergence policy framework, and compiling a National Information Infrastructure database
    - Offers a publicly accessible online NII database, providing information on related topics by country or key indicator

❑ **China-Japan-Korea (CJK)**

- Formed several working groups focusing on promoting harmonization and cooperation in ICT policy between three parties (the People’s Republic of China, Japan, and the Republic of Korea)
- Its work plan includes projects on network and information security policies and mechanisms, joint response to cyber attacks (including hacking and viruses), information exchange on online privacy protection information, and creation of a Working Group to promote this cooperation

Regional Intergovernmental Organizations – *Europe*

❑ **European Committee for Standardization (CEN)**

- A non-profit technical organization supporting the objectives of the European Union and the European Economic Area
- Has done much to contribute to the Information Society throughout Europe. In particular, CEN has provided significant work on security, trust, and data protection through completed focus groups on e-Business, e-Invoicing, digital rights management (DRM), network and information security (NIS), and e-Health, as well as current focus groups on biometrics, e-Government, and cultural diversity
- In addition, CEN is currently working on the second phase of a Data Protection and Privacy Workshop, Anti-Counterfeiting: Protocols for Detection of Counterfeits, a Cyber ID Workshop, and Information System for Disaster and Emergency Management

❑ **Council of Europe (COE)**

- Comprised of forty-seven member countries, one applicant country, and five observer countries (including the United States, Japan, Mexico, Canada, and the Holy See). Through promotion of the Convention on Cybercrime, the Council seeks to pursue a common criminal policy aimed at the protection of society against cybercrime
- The Council has also called on the need for a secure Information Society in the fight against terrorism and organized crime, the protection of children against sexual exploitation and sexual abuse, and the protection of human rights and fundamental freedoms, including the protection of personal data
- Organized several regional and international workshops and conferences on emerging cyber security issues, such as data privacy, identity theft, freedom of information, and cybercrime legislation

❑ **European Telecommunication Standards Institute (ETSI)**

- A not-for-profit organization that produces globally-applicable standards for Information and Communications Technology (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies
- ETSI has contributed numerous ICT security standards to the Information Society in the past few years

Regional Intergovernmental Organizations – *Europe*

❑ **European Union (EU)**

- The largest governing body within Europe and represents twenty-seven European countries
- Issued a Communique on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, and another related Communique on Network and Information Security
- The Commission also set forth a comprehensive strategy to embrace specific network and information security measures, a regulatory framework for electronic communications, and the fight against cybercrime
- Also developing numerous research programs, reports, publications, and metrics on ICT trust and security, secure network infrastructures, identity management, and critical infrastructure protection. The EU has also placed considerable emphasis on the fight against spam
- The Commission created the Contact Network of Spam Authorities (CNSA) in an effort to share information on current spam fighting practices with national authorities
  - ➢ **European Law Enforcement Organization (Europol)**
    - ○ The European Union's criminal intelligence agency. **Its primary contribution to cybercrime prevention was the creation of The Europol Computer System (TECS),** deployed in 2005 to facilitate sharing and analysis of criminal data between EU members and law enforcement organizations in other countries
  - ➢ **European Union Contact Network of Spam Authorities (CNSA)**
    - ○ In the CNSA, information on current practices to fight spam is exchanged between National Authorities, including best practices for receiving and handling Complaint information and Intelligence and investigating and countering spam. The CNSA has set up a cooperation procedure that aims to facilitate the transmission of complaint information between National Authorities

❑ **European Network and Information Security Agency (ENISA)**

- The European Union formed the European Network and Information Security Agency (ENISA) as a designated Center of Excellence on Network and Information Security (NIS)
- The agency is focused on three primary areas: awareness-raising, communication between members, and data collection and prevention
- Serves as a central data storage group for security incidents and other emerging risks within Europe and has a central role in coordinating communication between regional CERTs, and has implemented a new website to tackle Emerging Risks

Regional Intergovernmental Organizations – *Europe*

❑ **ICT Standards Board (ICTSB)**

- A collaborative group of organizations concerned with standardization and related activities in information and communications technologies, and its principal objective is to support an effective standardization system in Europe through various project teams and working groups

❑ **National Policing Improvement Agency (NPIA)**

- Created in 2007 to support police force operations throughout Europe. In particular, NPIA has a division dedicated to High Tech Crime, with programs designed to ensure that police staff are equipped with the knowledge and skills to meet the challenges set by criminals who use technology unlawfully
- With a heavy focus on training and education in cybercrime for law enforcement, NPIA offers a Masters in Cybercrime Forensics program and a First Responder e-Learning course for interested officers, as well as a diverse set of related courses on Internet forensics, network investigations, mobile phone forensics, identifying and tracing electronic suspects, and the role of technology in child abuse and economic crime investigations
- NPIA also hosts frequent conferences and workshops on high tech crime for national and international law enforcement agencies

❑ **Organization for Security and Co-operation in Europe (OSCE)**

- The world's largest security organization, consisting of fifty-six states in Europe, Central Asia, and America
- Organized workshops which provided a means to exchange best practices and encourage international legal cooperation. The ATU also organized national training workshops for prosecutors, judges and judicial officials on issues of extradition and mutual legal assistance in criminal matters, in particular those related to terrorism

❑ **Trans-European Research and Education Networking Association (TERENA)**

- A collaborative organization whose core business is to bring together managers, technical specialists and other people in the research networking community with their counterparts from other countries in Europe, mobilizing the expertise and experience of hundreds of professionals in the research and education networking area
- The objectives of TERENA are to promote and develop high-quality international network infrastructures to support European research and education
  - ➢ **European Task Force on Computer Security Incident Response Teams (TF-CSIRT)**
    - ○ One of TERENA's task forces and represents major initiatives by the European region with regard to Computer Security Incident Response Teams (CSIRTs) creation and communication
    - ○ Provides a forum where members of the European Union and neighboring countries can exchange CSIRT experiences and knowledge in a secure environment

Private-Public and Non-Governmental Organizations

Private-Public & Non-Governmental Organizations

❑ **Advocacy Groups**

- ➢ Anti-Phishing Working Group (APWG)
- ➢ Anti-Spyware Coalition (ASC)
- ➢ Coalition Against Unsolicited Commercial E-mail (CAUCE)
- ➢ European Spambox Project, The (SPOTSPAM)
- ➢ International Botnet Task Force (BTF)
- ➢ London Action Plan (LAP)
- ➢ Messaging Anti-Abuse Working Group (MAAWG)
- ➢ Spamhaus Project
- ➢ StopSpamAlliance (SSA)

❑ **Incident Response**

- ➢ Computer Emergency Response Team/Coordination Center (CERT/CC)
- ➢ Forum of Incident Response and Security Teams (FIRST)

❑ **Policy, Education, & Public Awareness**

- ➢ Authentication and Online Trust Alliance (AOTA)
- ➢ Global Information Infrastructure Commission (GIIC)
- ➢ International Chamber of Commerce (ICC)
- ➢ International Federation for Information Processing (IFIP)
- ➢ International Multilateral Partnership Against Cyber Threats (IMPACT)
- ➢ Open Information Systems Security Group (OISSG)
- ➢ Society for the Policing of Cyberspace (POLCYB)
- ➢ SysAdmin, Audit, Network, Security Institute (SANS)
- ➢ World Information Technology and Services Alliance (WITSA)
  - ❖ Global Internet Project (GIP)
- ➢ Family Online Safety Institute (FOSI)

❑ **Research, Development, & Standardization**

- ➢ 3rd Generation Partnership Project (3GPP)
- ➢ Central and Eastern European Networking Association (CEENet)
- ➢ Cooperative Association for Internet Data Analysis (CAIDA)
- ➢ GSM Association (GSMA)
- ➢ Institute of Electrical and Electronics Engineers (IEEE)
- ➢ International Organization for Standardization (ISO)
- ➢ Internet Research Task Force (IRTF)
- ➢ Internet Society (ISOC)
- ❖ Internet Engineering Task Force (IETF)
- ➢ Organization for the Advancement of Structured Information Standards (OASIS)
- ➢ Trans-European Research and Education Networking Association (TERENA)
- ➢ World Wide Web Consortium, The (W3C)

Private-Public and Non-Governmental Organizations – *Advocacy Groups*

❑ **Anti-Phishing Working Group (APWG)**

- A volunteer law enforcement association focused on eliminating the fraud and identity theft that results from phishing, pharming, and email spoofing of all types
- The APWG's most significant impact has been its participation in and presentations to ongoing regional and international conferences throughout the year

❑ **Anti-Spyware Coalition (ASC)**

- Dedicated to building a consensus about definitions and best practices in the debate surrounding spyware and other potentially unwanted technologies
- Provides numerous anti-spam resources on its website

❑ **Coalition Against Unsolicited Commercial E-mail (CAUCE)**

- A consumer advocacy group of volunteers, originally formed to encourage the creation of anti-spam legislation
- By distributing information and organizing member meetings, the CAUCE groups attempt to raise public awareness on spam-related issues
- In addition, the main CAUCE website contains helpful links and postings on news and current events related to the global fight against spam

❑ **European Spambox Project, The (SPOTSPAM)**

- Derived in September 2005 from the European Commission's Safer Internet Programme (EU)
- Was a twenty-four month contracted pilot project intended to facilitate legal action against spammers at the international level by drawing up self-regulatory strategies which can help protect end users against spam

❑ **Spamhaus Project**

- A non-profit organization dedicated to tracking Internet spam gangs and the mitigation of spam effects using real-time, spam-blocking databases made available to both administrators and general users.
- Spamhaus also maintains a database of collated information and evidence on known spam operations that have been terminated by a minimum of three ISPs for spam offenses (known as ROKSO, the Register of Known Spam Operations). Spamhaus made available to law enforcement agencies a special version of ROKSO that contains records with evidence, logs, and information on illegal activities

Private-Public and Non-Governmental Organizations – *Advocacy Groups*

❑ **International Botnet Task Force (BTF)**

- A worldwide coalition of public and private sector computer security specialists who share best practices, tools, and training to combat botnets and ultimately to assist law enforcement in prosecuting
- Aside from its training regimen, the organization joined with the FBI and Carnegie Mellon University to carry out Operation Bot Roast, an ongoing initiative to thwart bot-herders and disrupt and dismantle their botnets

❑ **London Action Plan (LAP)**

- An international effort of government and public agencies from twenty-seven countries to improve cooperation in spam law enforcement. It involves the combined efforts of OECD, the ITU, EU, APEC, and many other organizations
- In periodic communications, such as quarterly conference calls, participants exchange and discuss information, including new developments and trends, new data, effective enforcement strategies, organizational initiatives, and training sessions

❑ **Messaging Anti-Abuse Working Group (MAAWG)**

- Its purpose is to bring the messaging industry together to work collaboratively and successfully address forms of messaging abuse such as messaging spam, virus attacks, and denial-of-service attacks
- To facilitate improved communication and cooperation among its member organizations, MAAWG launched the MAAWG Abuse Contact Database, a database of email contacts that provides members with direct access to appropriate contacts at other MAAWG companies to assist in resolving various issues, such as reputation, malware, and fraud

❑ **StopSpamAlliance (SSA)**

- A cooperative international effort whose objective is to help coordinate international action against spam and related threats more effectively by gathering information and resources to improve information sharing among participating entities
- The StopSpamAlliance serves primarily as a central event and information notification mechanism for member organizations and visitors, as its website is filled with current news on upcoming conferences, summits, and meetings regarding cyber security and spam

Private-Public and Non-Governmental Organizations – *Incident Response*

❑ **Computer Emergency Response Team/Coordination Center (CERT/CC)**

- A group of trained security experts that investigate security breaches, evaluate cyber defenses, and analyze the state of information security within its corresponding area of jurisdiction
- Today, there are numerous CERTs and CSIRTs worldwide, working both independently and in collaboration to address cyber security incidents and promote awareness

❑ **Forum of Incident Response and Security Teams (FIRST)**

- An international confederation of 195 CSIRT teams from forty-three countries that have combined resources to share information and promote incident prevention in the international ICT community
- The organization promotes international cooperation by hosting conferences for nonmembers, encouraging the development of CSIRTs, and sharing technical information, tools, methodologies, and best practices
- FIRST maintains an extensive library of guides and publications based on material submitted by organization members, designed to assist both members and the general public in configuring systems securely according to configuration templates and security guidelines

Private-Public and Non-Governmental Organizations – *Policy, Education, & Public Awareness*

❑ **Authentication and Online Trust Alliance (AOTA)**

- A non-profit corporation seeking to create a trusted ecosystem and to foster the elimination of email and Internet fraud, abuse, and data intrusions, thereby enhancing online trust, confidence, and online protection of businesses and consumers through facilitation of best practices, data sharing, implementation of online trust solutions, and promotion of online safety worldwide

❑ **Global Information Infrastructure Commission (GIIC)**

- A confederation of chief executives and other officers of business firms engaged in the development, manufacture, deployment, operation, modernization, financing, and use of services and products based upon information and communication technologies
- Addressed the issues of identity management and end-user security, encouraged businesses to continue the development of security technologies for electronic commerce, and called for government support of private sector research and development in the field of security technology

❑ **International Chamber of Commerce (ICC)**

- An organization of businesses and is often a policy making body in such areas as anticorruption, banking techniques and practices, e-business, and ICTs
- With regard to cyber security, the ICC's Commission on E-Business, IT, and Telecoms (EBITT) includes the Task Force on Security and Authentication which provides several resources online for businesses to use in promoting secure ICTs

❑ **International Federation for Information Processing (IFIP)**

- A nongovernmental, non-profit umbrella organization devoted to ICT and science, and provides for the exchange of ideas, information, and experience by sponsoring more than one hundred conferences annually, and is divided into fourteen Technical Committees. Technical Committee Eleven (TC11) is the Security and Protection in Information Systems Committee, and has established a number of working groups, each devoted to a specific area of interest in security

❑ **SysAdmin, Audit, Network, Security Institute (SANS)**

- The most trusted and the largest source for information security training and certification in the world, and reaches more than 165,000 security professionals around the world
- SANS maintains a wealth of knowledge and resources on nearly all aspects of information security and manages the Internet Storm Center – the Internet's early warning system and offers a variety of training courses in information security

Private-Public and Non-Governmental Organizations – *Policy, Education, & Public Awareness*

❑ **International Multilateral Partnership Against Cyber Threats (IMPACT)**

- A new private-public organization based in Cyberjaya, Malaysia that, in collaboration with the ITU, seeks to bring together key personnel in world governments, academia, and the private sector for the purpose of combating cyber-terrorism
- Projects: held inaugural IMPACT World Cyber Security Summit (WCSS) In Kuala Lumpur, Malaysia. This was the largest ministerial-level forum ever organized on cyber-terrorism and security

❑ **Open Information Systems Security Group (OISSG)**

- An independent, non-profit organization seeking to spread information security awareness by creating an environment where security enthusiasts from around the world can share and build knowledge
- OISSG conducts research in several security fields and holds worldwide conferences and presentations to raise the level of information security awareness and to teach advanced security practices developed by OISSG

❑ **Society for the Policing of Cyberspace (POLCYB)**

- A non-profit organization that works to promote information sharing, public education on information protection and Internet safety, and public awareness on cybercrime through Quarterly and Annual General Meetings, international conferences, and public education forums
- In addition, the Cyber-Pol website includes numerous links and other resources related to cybercrime and information security awareness

❑ **World Information Technology and Services Alliance (WITSA)**

- A consortium of over sixty information technology industry associations from economies around the world
- Dedicated to promoting the growth and development of the industry through appropriate public policy, international trade and investment, the sharing of knowledge and experience, and the exchange of information
- With particular relevance to cyber security, WITSA has a Task Force on Electronic Commerce and a Task Force on Critical Information Infrastructure. WITSA is known for two flagship events, held once every two years in different nations: The Global Public Policy Conference (GPPC) and The World Congress on Information and Technology (WCIT)

➢ **Global Internet Project (GIP)** Advisory Committee to WITSA

- ○ An independent, non-partisan, international group of senior executives committed to fostering continued growth of the Internet
- ○ Contains numerous online resources on information security, including original publications, information on initiatives and events, and links to documents from other notable organizations and companies

Private-Public and Non-Governmental Organizations – *Policy, Education, & Public Awareness*

❑ **Family Online Safety Institute (FOSI)**

- Is an International, non-profit membership organization that works to make the online world safer for kids and their families by identifying and promoting best practice, tools and methods in the field of online safety, that also respect free expression
- There are four pillars to the work of the Institute: events, public policy, technology and education
- Its offices are located in the US and the UK. Current members include: AOL, AT&T, Blue Coat, Boodoo, British Telecom, Comcast, CompTIA, Facebook, France Telecom, Google, GSM Association, Loopt, Microsoft, MySpace, NCTA, Ning, Nominum, Optenet, Kingston Communications, Privo, RuleSpace, Sprint, StreamShield, Symantec, Telefónica, Telmex, The Wireless Foundation, Verizon and Yahoo!
- Held a comprehensive list of events, including:
  - ➢ Internet Governance Forum (IGF) Meetings
  - ➢ 3 Annual Conferences and Exhibitions
  - ➢ FOSI European Conference (16 September 2009, Paris)
  - ➢ GSMA/FOSI Roundtable: Mobile Safety and Broadband Responsibility for All (17-18th June 2009, London)
  - ➢ Wireless Online Safety: Keeping Kids Safe in a Mobile Environment (22 April 2009, Washington DC)
- Publishes a bi-monthly newsletter called “InSight”. It's designed to keep FOSI’s members and those that support its mission up-to-date with the latest news, events and initiatives. Latest editions or back copies can be download from the website
- **ICRA** – www.icra.org (formerly the Internet Content Rating Association) is part of the Family Online Safety Institute; The centerpiece of this organization is the descriptive vocabulary, often referred to as "the ICRA questionnaire." Content providers check which of the elements in the questionnaire are present or absent from their websites. This then generates a small file containing the labels that is then linked to the content on one or more domains. Users, especially parents of young children, can then use filtering software to allow or disallow access to web sites based on the information declared in the label
- In November 2009, FOSI signed a Memorandum of Understanding with the Suzanne Mubarak Women’s International Peace Movement and the Ministry of Communications and Information Technology of the Arab Republic of Egypt. This agreement commits FOSI and the Egyptian Government to a collaborative partnership in promoting family online safety over the next two years. The commitment includes joint efforts to promote digital citizenship in Egypt and the Arab world, assistance from the Cyber Peace Initiative for FOSI’s online safety education initiatives, plans for a workshop in Egypt with the Cyber Peace Initiative to showcase current protection tools and identify online safety technology trends, and FOSI’s representation on the Cyber Peace Initiative International Executive Board

Private-Public and Non-Governmental Organizations – *Research, Development, & Standardization*

□ **3rd Generation Partnership Project (3GPP)**

- A collaboration of international telecommunications standards bodies created in 1998 to produce globally applicable Technical Specifications and Technical Reports for a 3rd Generation Mobile System based on evolved GSM core networks and the radio access technologies that they support
- Performs analyses of potential security threats to the system, considers the new threats introduced by the IP based services and systems, and sets the security requirements for the overall 3GPP system
- Maintains a comprehensive website listing of technical 3GPP security specifications
- Hosted a wealth of working group meetings in various countries around the to discuss such topics in 3GPP security research

□ **Central and Eastern European Networking Association (CEENet)**

- A non-profit partnership of over twenty national research and education networks working to coordinate the international aspects of the academic, research, and education networks in Central and Eastern Europe and in adjacent countries
- CEENet's work is typically accomplished through conferences, workshops, and courses in network technology, publications, promotion of national network services, exchange of technical information to research networks, and formation of working parties to undertake relevant technical activities

□**GSM Association (GSMA)**

- Represents over eighty-six percent of the world's mobile phone connections and works to ensure mobile phones and wireless services work globally and are easily accessible, enhancing their value to individual customers and national economies, while creating new business opportunities for operators and their suppliers
- GSMA has an extensive mobile fraud and security program, including research and development on mobile application security (MAS) and GSM security algorithms
- GSMA has also developed several mobile security algorithms used to provide authentication and radio link privacy to users on a GSM network
- GSMA also manages the Security Accreditation Scheme (SAS), a voluntary audit program for GSM suppliers to validate the comprehensive security of their production sites and processes, benefiting both suppliers and network operators
- The GSMA Certified Fraud Training programme was launched in May 2005 to give the most up-to-date skills and knowledge to those whose job it is to detect fraudulent activity and to minimize its financial impact on an operator's business

Private-Public and Non-Governmental Organizations – *Research, Development, & Standardization*

❑ **Institute of Electrical and Electronics Engineers (IEEE)**

- A non-profit organization created to advance the theory and application of electrotechnology and allied sciences; serve as a catalyst for technological innovation; and support the needs of its members through a wide variety of programs and services
- The IEEE Computer Society's Technical Committee on Security and Privacy (TCSP) hosts many workshops and conferences on ICT security and privacy, including most notably the IEEE Symposium on Security and Privacy and the Computer Security Foundations (CSF) Symposium
- The TCSP CSF Symposium is also held annually for researchers in computer security to examine current theories of security

❑ **International Organization for Standardization (ISO)**

- A nongovernmental organization and network of national standards institutes from 157 countries
- Forms a bridge between the public and private sectors to develop and publish the world's largest repository of International Standards

❑**Internet Society (ISOC)**

- A non-profit organization that provides leadership in Internet-related standards, education, and policy
- Works to promote a secure Internet infrastructure by facilitating discussions on key policy decisions and initiatives towards self-government of the Internet through debate and development of position papers, white papers, and statements on Internet security related issues
- ISOC's most notable information security event is the annual Network and Distributed System Security Symposium (NDSS), held in San Diego, California, in February of each year, bringing together a large group of security researchers, implementers, and experts to learn about and discuss cutting-edge advances in the science and application of network and distributed systems security
- The ISOC-EMEA (Europe, Middle East, and Africa) Security Expert Initiative (SEINIT), completed in 2006, was a two-year contract sponsored by the European Commission to address the areas of security and privacy within the context of the IPv6 protocol. At the end of the two years, the SEINIT project had successfully developed a trusted, dependable, inter-operable, and ubiquitous security framework for next generation Internet infrastructures

➢ **Internet Engineering Task Force (IETF)**

- ○ Produces high quality, relevant technical and engineering documents that influence the way people design, use, and manage the Internet in order to improve its functionality

Private-Public and Non-Governmental Organizations – *Research, Development, & Standardization*

❑ **Cooperative Association for Internet Data Analysis (CAIDA)**

- A collaboration of private and public organizations working to promote research on global ICT-based challenges and develop useful tools and strategies for Internet Service Providers and other relevant stakeholders within the industry

❑ **Internet Research Task Force (IRTF)**

- Created to promote research of importance to the evolution of the future Internet by creating focused, long-term and small Research Groups working on topics related to Internet protocols, applications, architecture and technology

❑ **Organization for the Advancement of Structured Information Standards (OASIS)**

- A non-profit consortium founded in 1993 consisting of over 5000 vendors and users from one hundred countries and representing over six hundred organizations committed to the development, convergence, and adoption of open standards for the information society
- Hosts two online information portals on XML and web services standards, Cover Pages and XML.org, both widely regarded by the online open security standards community
- Co-sponsors educational conferences and seminars and works to develop security standards needed in e-business and Web services applications

❑ **Trans-European Research and Education Networking Association (TERENA)**

- A forum that provides an environment for fostering new initiatives in the European research networking community
- Supports joint European work in developing, evaluating, testing, integrating and promoting new networking, middleware and application technologies through the TERENA
- Organizes conferences, workshops, and seminars for the exchange of information in the European research networking community, and pursuing knowledge transfer to less advanced networking organizations

❑ **World Wide Web Consortium, The (W3C)**

- An international consortium of public and private organizations devoted to leading the World Wide Web to its full potential by developing protocols and guidelines that ensure long-term growth for the Web
- Engages in education and outreach, develops software, and serves as an open forum for discussion about the Web
- Currently focuses on security research and development of security standards

Selected Country-Specific Organizations

USA

❑ **National Cyber Security Division**

- The National Cyber Security Division (NCSD) works collaboratively with public, private and international entities to secure cyberspace and America's cyber assets
- **Organization and Functions:** NCSD works to achieve its strategic objectives through the following programs:
  - ➢ ***National Cyberspace Response System:*** The National Cyber Security Division seeks to protect the critical cyber infrastructure 24 hours a day, 7 days a week. The National Cyberspace Response System coordinates the cyber leadership, processes, and protocols that will determine when and what action(s) need to be taken as cyber incidents arise. Examples of current cyber preparedness and response programs include:
    - ❖ **Cybersecurity Preparedness and the National Cyber Alert System**: Cyber threats are constantly changing. Both technical and non-technical computer users can stay prepared for these threats by receiving current information by signing up for the National Cyber Alert System
    - ❖ **US-CERT Operations**: US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities
    - ❖ **National Cyber Response Coordination Group** : Made up of 13 federal agencies, this is the principal federal agency mechanism for cyber incident response. In the event of a nationally significant cyber-related incident, the NCRCG will help to coordinate the federal response, including US-CERT, law enforcement and the intelligence community
    - ❖ **Cyber Cop Portal**: is an information sharing and collaboration tool accessed by over 5,300 investigators worldwide who are involved in electronic crimes cases
  - ➢ ***Cyber Risk Management Programs:*** Through Cyber Risk Management, the National Cyber Security Division seeks to assess risk, prioritize resources, and execute protective measures critical to securing our cyber infrastructure. Examples of current cyber risk management programs include: Cyber Exercises, National Outreach Awareness Month, and Software Assurance Program

❑ **The National Cyber Security Alliance:** NCSA's mission is to empower and support digital citizens to use the Internet securely and safely, protecting themselves and the cyber infrastructure. NCSA seeks to raise awareness of cyber security to the level of other cultural messaging that is universally good for citizens—healthy eating, exercise, and safe driving—by teaching skills and judgment to build a national understanding about appropriate online tools and behavior. NSCA's public facing presence is its website www.staysafeonline.org

❑ **The U.S. Cyber Consequences Unit:** The U.S. Cyber Consequences Unit (US-CCU) is an independent, non-profit research institute. It provides assessments of the strategic and economic consequences of possible cyber-attacks and cyber-assisted physical attacks. It also investigates the likelihood of such attacks and examines the cost-effectiveness of possible counter-measures

Australia

❑ **The Australian Government Computer Emergency Readiness Team (GovCERT.au)**

- Established to help formulate cyber security policy and to liaise with foreign government computer emergency response teams (CERTs)
- Assists in coordinating Australian Government policy for computer emergency preparedness, response, readiness and recovery in relation to Australia's critical infrastructure and key business. GovCERT.au is responsible for providing advice and information to help owners and operators of critical infrastructure and key business secure their networks and systems
- Is the point of contact within the Australian Government for foreign governments on CERT issues impacting on Australia's critical infrastructure and key business, and coordinates any related requests
- Is the Australian Government lead on issues related to supervisory control and data acquisition and control systems security. GovCERT.au receives cyber security information for distribution to Australian businesses, including critical infrastructure owners and operators

❑ **The New National Computer Emergency Response Team, or CERT Australia**

- Is the national coordination point for providing cyber security information and advice to all Australians and the initial point of contact for international agencies to let Australia know about cyber security issues
- Works with other national CERTs around the world, the IT industry and Australian Internet Service Providers to help network operators identify and respond to cyber security incidents
- Builds on the work of the Australian Government Computer Emergency Readiness Team, or GovCERT.au – currently helping owners and operators of critical infrastructure secure their networks and systems

❑ **The Cyber Security Operations Centre, in the Defense Signals Directorate**

- Provides Government with enhanced situational awareness about cyber security
- Maintains a 24/7 watch on cyber security activities that might threaten Australia's national security and coordinates responses to cyber security incidents of national importance

❑ **Stay Smart Online (http://www.staysmartonline.gov.au/)**

- Provides all Australian online users with information on the simple steps they can take to secure themselves online. This includes information and advice on how to secure your computer and your transactions online
- Includes an E-security Alert Service which is a free subscription based service that provides home users and small to medium enterprises with information on the latest computer network threats and vulnerabilities in easy to understand language. It also provides solutions to help manage these risks

Japan

- ❑ **Japan Computer Emergency Response Team Coordination Center, JPCERT/CC**
  - Is the first CSIRT (Computer Security Incident Response Team) established in Japan
  - Coordinates with network service providers, security vendors, government agencies, as well as the industry associations. As such, it acts as a "CSIRT of CSIRTs" in the Japanese community
  - In the Asia Pacific region, JPCERT/CC helped form APCERT (Asia Pacific Computer Emergency Response Team) and provides a secretariat function for APCERT. Globally, as a member of the Forum of Incident Response and Security Teams (FIRST), JPCERT/CC coordinates its activities with the trusted CSIRTs worldwide
  - Its activities include: Incident Response and Analysis, Security Alert, Coordination with other CSIRTs, Vendor Coordination, Education & Training, and Research & Analysis

- ❑ **The Information-technology Security Center (IPA ISEC)**
  - Designed to:
    - ➢ Assuring the security and reliability of IT in the social infrastructure
    - ➢ Strengthening international competitiveness
    - ➢ Cultivating highly skilled world-class IT human resources

- ❑ **Japan Information Processing Development Center (JIPDEC)**
  - Performs the following Activities:
    - ➢ Privacy, Security and Information Management
    - ➢ Research and International Cooperation
    - ➢ Information Technology Training
    - ➢ Information Technology Development
    - ➢ Electronic Commerce (including Electronic Data Interchange)

Canada, New Zealand, & UK

❑ **Canadian Cyber Incident Response Centre (CCIRC)**

- Is responsible for monitoring threats and coordinating the national response to any cyber security incident. Its focus is the protection of national critical infrastructure against cyber incidents
- Its responsibilities include:
  - ➢ Emergency management
  - ➢ National security
  - ➢ Crime prevention
  - ➢ Law enforcement policy
  - ➢ Corrections policy
- Works closely with the following organizations to monitor international cyber threats and share information on best practices for protecting critical infrastructure: GovCERT (Australia), CCIP (New Zealand), US-CERT (United States), and CPNI (UK)

❑ **The Centre for Critical Infrastructure Protection (CCIP)**

- Is dedicated to improving the protection and computer security of New Zealand's Critical National Infrastructure (CNI) from cyber based threats
- Provides 24/7 watch and warning advice to the owners and operators of our CNI and the New Zealand Government
- Investigate and analyses cyber incidents that occur against New Zealand's CNI
- Works with CNI protection agencies both nationally and internationally to improve the awareness and understanding of cyber security in New Zealand

❑ **Center for the Protection of National Infrastructure (CPNI UK)**

- Is the government authority that provides protective security advice to businesses and organizations across the national infrastructure
- CPNI advice is targeted primarily at the critical national infrastructure (CNI) - those key elements of the national infrastructure which are crucial to the continued delivery of essential services to the UK
- CPNI takes the lead for providing protective security advice to the national infrastructure within Northern Ireland, particularly relating to the delivery of advice to CNI operators covering physical, personnel and information security

Arab Organizations

Arab Organizations

- ❑ **Tunis**
  - ➢ Computer Emergency Response Team Tunisian Coordination Center (CERT-TCC)

- ❑ **Egypt**
  - ➢ The Egyptian Computer Emergency Response Team (CERT)
  - ➢ Youth Internet Safety Focus Group (Net-Aman)
  - ➢ The Commission for Protection of User Rights
  - ➢ Cyber Peace Initiative

- ❑ **UAE**
  - ➢ The UAE National Computer Emergency Response Team (aeCERT)
  - ➢ ETISALAT Computer Emergency Response Team (ETISALAT-CERT)

- ❑ **KSA & Qatar**
  - ➢ Computer Emergency Response Team (CERT-SA)
  - ➢ Qatar’s Center for Information Security (Q-CERT)

- ❑ **Regional**
  - ➢ Gulf Cooperation Council (GCC)
  - ➢ League of Arab States
    - ❖ The Arab Information and Communication Technologies Organization (AICTO)
  - ➢ Pan Arab Observatory for Cyber Security

Arab Organizations – *Tunis*

- ❑ **Computer Emergency Response Team - Tunisian Coordination Center (CERT-TCC)**
  - A public CSIRT hosted by the National Agency for Computer Security, and was established in 2004
  - Increases awareness and understanding of information security and computer security issues throughout the two communities of professionals and citizens and initiates proactive measures
  - Provides a reliable, trusted, 24 hours and 7days/week, single point of contact for emergencies, in order to help security incidents and ensure protection of the national cyber-space and the continuity of national critical services in spite of successful attacks or failures
  - Provides a high level of training and certification for trainees and professionals
  - Informs about best practices and about security organizational aspects, with a special focus on audit and risk management
  - Informs about vulnerabilities and corresponding response and serves as a trusted point of contact for collecting and in a future step identifying vulnerabilities in computer systems
  - Informs about security mechanisms and tools, including those available from the open-source field and ensures that appropriate technology and best management practices are used
  - Implements mechanisms that enable quick alerting and response actions and help organizations and institutions to develop their own incident management capabilities
  - Facilitates communication among professional and experts working in the security field and build relationships and stimulates cooperation among and across governmental agencies, public/private businesses, and academic organizations
  - Collaborates with the international and national community in detecting and resolving computer security incidents
  - Promotes or undertakes the development of education, awareness and training materials appropriate for a variety of different audiences to further improve the skills and technical knowledge of IT users and security professionals

Arab Organizations – *Egypt*

❑ **The Egyptian Computer Emergency Response Team (CERT)**

- Is responsible for dealing with online threats and emergencies, and was launched in April 2009
- Is in charge of incident handling, awareness and security alerts, international coordination, and training and capacity building

❑ **Youth Internet Safety Focus Group (Net-Aman)**

- Increases awareness and helps children and young people identify harmful content and deal with it

❑ **The Commission for Protection of User Rights**

- Conducting a survey with Internet users to improve the quality of service provided to the user
- Providing awareness to telecom users about positive usage of internet
- Encouraging service providers to implement internet filters
- Coordinating between concerned parties and internet provider

❑ **Cyber Peace Initiative**

- Operates under the Youth Unit of Suzanne Mubarak's Women's International Peace Movement
- The initiative, which is the first of its kind in the region, is a means to empower the use of ICT to spread a culture of peace, tolerance, understanding and dialogue among youth. It also aims to protect the children from the misuse of the internet
- Holds monthly awareness meetings with youth
- Identifies and promotes Internet safety tips to parents, youth and children, as well as explains the pros and cons of different Internet based IT tools
- Identifies and allies with key international organizations and NGOs active in the field, e.g. The International Center for Missing and Exploited Children (ICMEC) and Child Exploitation and Online Protection Center, to tailor solutions for different societies, attending and hosting forums as appropriate
- Meets periodically with heads of NGOs for raising awareness and discussion of issues
- Produces a code of ethics for young users
- Promotes a system of classification, tools, and filters

Arab Organizations – *UAE*

- ❑ **The UAE National Computer Emergency Response Team (aeCERT)**
  - The cyber security coordination center in the UAE. It was established by the Telecommunications Regulatory Authority (TRA) as an initiative to facilitate the detection, prevention and response of cyber security incidents on the Internet
  - Provides coordination and advisory services on mitigating cyber security risks
  - Its current services include providing advice and education as well as alerting to threads and communications, incident handling and response, and research and analysis related to concerned topics
  - One of the major achieved activities is the "protecting your online identity" national awareness campaign that addresses the issues of Information Security Essentials, Password Security and Social Engineering
  - Launched its awareness campaign – 'Towards a safe cyber culture" with SALIM – the cyber security advisor. SALIM was born in the aeCERT to spread a safe cyber culture by giving simple and easy-to-use tips and advices, in order to build a promising generation that has an integrated knowledge about information security
- ❑ **ETISALAT Computer Emergency Response Team (ETISALAT-CERT)**
  - The Computer Emergency Response Team of the Emirates Telecommunications Corporation - ETISALAT
  - Its purpose to achieve continuous and improved information technology orientated security service, which is both proactive and reactive; to serve its constituency to prevent or recover from network based cyber-attacks of all forms

Arab Organizations – *KSA & Qatar*

❑ **Computer Emergency Response Team (CERT-SA)**

- Is a non-profitable center established to play an important role in increasing and cultivating awareness, knowledge, management, detection, prevention, coordination and response to information security incidence at the national level
- Its services include:
  - ➢ Awareness Building, Education/training
  - ➢ Security Related Information Dissemination, Alerts and Warning
  - ➢ Incident Response Support & Incident Analysis
- Features a Resource Center that provides guidance designed to help IT professionals address security issues commonly seen in an enterprise or business as well as some useful security tools (e.g. database security, mobile security, operating system security, etc.)

❑ **Qatar’s Center for Information Security (Q-CERT)**

- Q-CERT, Qatar's center for information security, was created by the Supreme Council for Information and Communications Technology (ictQATAR) to safeguard and improve the security of information and communications systems
- Q-CERT works with government agencies, businesses, and the citizens of Qatar to address cyber security risks, protect sensitive information, and ensure the safety of our children on the Internet
- Works with public and private schools to hold training workshops for teachers and students to raise awareness on the safe use of the internet
- Its activities include Creating a site on the government portal that is dedicated to the education of children and their parents concerning security risks and vulnerabilities, and to report online security problems which may raise in cyberspace
- Actively participates with the International Telecommunications Union in its efforts to develop an initiative to protect children online

Arab Organizations – *Regional*

❑ **Gulf Cooperation Council (GCC)**

- Calls for the adoption of a Treaty by the States of the Gulf Cooperation Council, inspired by the Council of Europe Convention on Cybercrime, to be expanded later to all Arab countries
- Invites all the GCC countries to adopt laws against cybercrime inspired from the model used by the UAE’s cybercrime law
- Calls for the adoption of laws that are suitable to procedural matters such as custody, inspection and other investigation procedures dedicated for these types of crimes

❑ **The Arab Information and Communication Technologies Organization (AICTO)**

- Is an Arab governmental organization working under the guidance of the League of Arab States
- Aims at developing ICTs throughout the Arab region and providing the necessary mechanisms to support cooperation and complementarities between AICTO members promote and enrich common policies and strategies to develop vital technological domains
- Encourages Arab and foreign ICT investment in the Arab region with further identification of investment opportunities, incentives and available encouragements and facilities in the field
- Disseminates information about Arab ICT solutions, innovations and software in order to market the relevant Arab production
- Participates in collecting, filing, and disseminating studies and research related to identifying Arab future needs in the field of ICT
- Organizes periodic exhibitions and conferences to inform about achievements and reinforce cooperation and partnership on the Arab level
- Promotes the exchange of ICT experts between Arab countries
- Future projects will be dealing with: E-content, Development and promotion of scientific research, Building capacity and e-education, and Cybersecurity

Arab Organizations – *Regional*

❑ **The Initiative for An Open Arab Internet (openarab.net)**

- An initiative by the Arabic Network for Human Rights Information (Anhri) advocating free use of the Internet without censorship, blocking or spying.
- Seeks to provide international and Arab information and internet related documents. The initiative also defends internet users, web-designers, and writers by organizing legal and media campaigns and highlighting practices restricting Internet freedom

❑ **Arab Intellectual Property Centre (www.arabipcentre.com)**

- An online portal launched by the League of Arab States, Microsoft Corp. and Khasawneh & Associates Legal Consultants (a member of KSLG) on September 27, 2009
- Aims to promote the protection of intellectual property by providing a central database on intellectual property and internet crime issues within the region, including an extensive collection of regional laws and regulations, international treaties and agreements and intellectual property case law from around the Middle East region
- Provides a central hub for best practice sharing and legal resources on intellectual property in the Arab region

Arab Organizations –
Pan Arab Observatory for Cybersecurity

Observatory Goals, Composition, Management, and Current Members

Observatory Goals:

- ❑ Produce a clear and consistent overview of the emerging cyber security needs of the Arab-Speaking society
- ❑ Produce a clear and consistent overview of the legal and regulatory framework that should be dealt with
- ❑ Create a solid and clear framework for different countries to reach harmony in their legal and regulatory matters to secure the cyberspace for the government and its citizens
- ❑ Cover the commercial, economic, academic and social aspects of cyber security

Observatory Composition:

The observatory gathers experts and professionals from various Cyber security sectors such as legal, information technology, telecommunications, sociology and internet services, economic community, public authorities, and authorities concerned directly with the development of E-Commerce and E-Government

Observatory Management:

The Observatory consists of two committees in charge of performing the work, following-up and coordinating the various efforts: **General Committee** and **Executive Committee**

Observatory Current Members:

- ❑ Ministry of Justice
- ❑ Ministry of Interior
- ❑ The Lebanese Association for Information Technology
- ❑ Telecommunications Regulatory Authority
- ❑ College of Engineering – Antonine University, Baabda
- ❑ Arab States League – Judicial and Legal Research Center
- ❑ Microsoft

Roles and Responsibilities

General Committee

❑ Includes local representatives from all concerned sectors in each country, without constraints of the number of members or the difference between one country and another

❑ Responsibilities include:

- developing a comprehensive plan of action
- development and implementation of monitoring, assessment and analysis processes
- identifying risks and proposing solutions and means of protection
- developing awareness plans as well as drafting and disseminating safety indicators
- coordinating the work between experts and academics
- formulating proposals and pursuing their implementation locally

Executive Committee

❑ Includes representatives from all participating Arab countries who are elected from the members of each country. Each participating country should have three members, at least

❑ Responsibilities include:

- developing a plan of action for each country
- implementing the action plan and policy of the General Authority, to the extent that is consistent with each country's plans and the proposals of the General Authority
- coordinating different efforts, and studying the various proposals and submitting them to the involved official bodies and specialized regional bodies

Proposed Structure – General Committee (1/2)

Should establish the working group and develop its regulatory framework, in line with the in-acted laws. The General Committee should be composed of three sub-committees:

- ❑ **Policy, Administrative, and Public Relations Sub-Committee:** is responsible for:
  - Establishing a network of relationships that provides adequate coverage of the various legislative, regulatory, administrative, security, academic and professional activities. This network should include the following:
    - Ministries of Interior, Defense, Justice, ICT, and Education
    - Major universities
    - Main Operators (ICT, Telecommunications)
  - Creating and regularly updating a website dedicated to the working group, responsible for issuing periodical updates on developments in the administrative, legislative, and regulatory areas. This website should constitute a communication platform between all members of the observatory, and between all those involved in cyber security and the proper engagement in the information society
  - Organizing workshops and scientific meetings, seminars, and training programs for professionals and ordinary citizens, in cooperation with official and private bodies
  - Developing comprehensive public awareness plans in the area of cyber security
  - Strengthening the cooperation between various bodies and sectors of society
  - Reviewing the curriculums for higher education as to the extent to which it responds to the needs of development, awareness, and the proper and safe engagement in the information society
  - Providing a widely available hotline as a mean to connect to the Observatory for Cyber Security. This should serve as a national center to disseminate information about threats, vulnerabilities, and cyber security incidents
- ❑ **Technical Sub-Committee:** is responsible for:
  - Following-up on safety standards and measures in the areas related to the use of information technology and communications
  - Following-up on the latest developments in internet management and communications, especially those that directly affect cyber security
  - Establishing databases about the standards and rules adopted in the field of information and system security, and the security of persons involved in various professional fields in both the public and private sector

Proposed Structure – General Committee (2/2)

- **Legal Sub-Committee:** is responsible for:
  - Following-up on the latest legislative and regulatory developments especially those that directly affect cyber security
  - Following-up on developments and news of violations of rights and freedom, and abuse to individuals and institutions in the Arab world
  - Following-up on cyber security issues, especially with respect to limiting violations, and prosecuting crimes
  - Establishing a regulatory and legislative database specialized in security and safety standards in the area of cyber security, so that everyone concerned can recognize the various legislative and regulatory rules, in an easy and reliable manner
  - Following-up and developing indicators that provide the legislative and regulatory framework, and the extent to which the various cyber security frameworks in the Arab region are in harmony
  - Studying various strategies on regulation and legislation, especially those related to e-government
  - Developing a report, in coordination with the Technical Sub-committee, on the status of cyber security in the Arab world, from the perspectives of available techniques as well as legal and regulatory means. This report should provide proposals to the various governments taking into account the need to enhance and develop digital transactions, electronic commerce, and the respect for the rights of citizens and the need to protect them from infringements on their financials and personal data
  - Reviewing the draft laws and regulations that are proposed in the Arab countries, and providing proposals which facilitate the harmonization between these laws

The above three sub-committees should work in coordination with other local, regional, and international bodies and organizations. At the forefront of these bodies are: the Arab States League, the United Nations, specialized research centers, state agencies, and the forces acting on the pursuit and suppression of cyber crimes

Proposed Structure – Executive Committee

Includes representatives from all participating Arab countries who are elected from the members of each country. This committee should serve as a link between the General Committee and member states. Each participating country should have three members, at least. Each of these three members should work with one of the following three sub-committees of which the Executive Committee is composed:

❑ **Legal Sub-Committee:** is composed of representatives from each member country. Each member should perform the following:
  - Provide reports and updates on the legal status and latest legislative developments within his country
  - Implement the recommendations and proposals for the harmonization between laws suggested by the General Committee in the legal field & translate them into local legal systems/rules, to the extent that is consistent with each country's plans/systems

❑ **Technical Sub-Committee:** is composed of representatives from each member country. Each member should perform the following:
  - Provide reports on technical data, standards, rules and statistics related to his country
  - Implement recommendations of the General Committee in the technical field & translate them into local best practices/rules

❑ **Public Relations/Administrative Sub-Committee:** is composed of representatives from each member country. Each member should perform the following:
  - Establish a local network in his country in order to stay up-to-date with the activities and recommendations of the General Sub-Committee, and provide coverage of the various activities related to cyber security within his country
  - Apply awareness plans and capacity building programs suggested by the General Committee

Suggested Arab countries, already having experience and taskforces in the area of cyber security, who should have members in the above Sub-Committees are: UAE, Qatar, Egypt, and Tunisia

Proposed Action Plan (1/2)

In addition to the previously mentioned responsibilities of each sub-committee, the following activities are also suggested:

❑ Identify and ally with key international organizations and NGOs active in the field, e.g. The International Center for Missing and Exploited Children (ICMEC) and Child Exploitation and Online Protection Center, to tailor solutions for different societies, attending and hosting forums as appropriate

❑ Meet periodically with heads of NGOs for raising awareness and discussion of issues to create a trickle down effect

❑ Produce a code of ethics for young users to be applied at national levels, and hold monthly awareness meetings with youth. These meetings should be directed at identifying and promoting Internet safety tips to parents, youth and children, as well as explaining the pros and cons of different Internet based IT tools

❑ Promote a system of classification, technical tools, standards, and filters

❑ Promote the building of national expertise in information security, incident management and computer forensics

❑ Establish an alerting mechanism that allows for timely delivery of new alerts and mitigation strategies

❑ Establish a guide for member countries to perform an exercise to assess preparedness capabilities in response to a cyber incident of national significance

❑ Coordinate with member states, universities and the private sector to produce a National Cyber security Awareness month

❑ Encourage the adoption of cyber ethics, cyber safety and cyber security in school education in the member countries, as well as teacher preparedness to address these issues in the classroom. Also, encourage the development of a volunteer program for computer security professionals to teach cyber security in schools

❑ Establish a an independent, non-profit research institute that provides assessments of the strategic and economic consequences of possible cyber-attacks and cyber-assisted physical attacks. It also investigates the likelihood of such attacks and examines the cost-effectiveness of possible counter-measures, and give professional opinion to forensic investigators within each member's local authority

Proposed Action Plan (2/2)

❑ Create helpful booklets in the area of cyber security. Suggestion: an Identity Theft Booklet that provides practical advice and strategies on how to protect personal and financial information, as well as information on computers and what to do if someone becomes a victim of identity theft. The booklet also includes a checklist to assess how vulnerable we are to identity crime and provides a list of government resources to help protect our personal information

❑ Maintain a large network of trusted CERT contacts around the world. These contacts should receive early warning of global threats and assist in responding to incidents which span jurisdictions

❑ Become a trusted member in related international organizations such as ITU, ISO, etc.

❑ Create a free alert service on the Observatory's website that provides easy to understand information on the latest e-security threats and vulnerabilities, a free interactive education resource for primary and secondary school students, videos with useful tips on protecting one's computer, a self assessment tool for small businesses, and information for parents

❑ Enhance the Arab World's regional and international cooperation on information security

❑ Facilitate information sharing and technology exchange, including information security, computer virus and malicious code among members of the observatory

❑ Promote collaborative research and development on subjects of interest to various members of the observatory

❑ Provide inputs and/or recommendations to help address legal issues related to information security and emergency response across regional boundaries

❑ Establish media coverage of the various activities of the observatory (publishing articles, interviews, flash news, workshops and events)

❑ Establish a central help desk and national help desks to respond to cyber security issues. This should work in coordination with local CERTs within each member country and local authorities

Thank You For Your Attention!

www.tra.gov.lb