

Connect Arab Summit
5-7 March 2012
Doha, Qatar

15 February 2012
Original: English

Building trust and security in the use of ICTs

Background Paper

1. BACKGROUND

The World Summit on the Information Society (WSIS) recognized the real and significant risks posed by inadequate confidence and security in the use of ICTs and the proliferation of cybercrime. Paragraphs 108-110 of the Tunis Agenda for the Information Society, including the Annex, set out a plan for multi-stakeholder implementation, at the international level, of the WSIS Plan of Action describing the multi-stakeholder implementation process according to eleven Action Lines and allocating responsibilities for facilitating WSIS implementation in the different Action Lines. During WSIS, world leaders and governments designated ITU to facilitate the implementation of WSIS Action Line C5, "Building confidence and security in the use of ICTs".

ICTs are part of everything we do in the modern world, and will continue to play an ever-increasing role in social and economic development as we move forward. ICTs have contributed businesses, governance, education, health, environment and communication more efficient. The digital revolution has changed how business is transacted and how governments operate. Globalization and technology advancement have made critical infrastructure vulnerable and thus a potential terrorist target. Countries face real risks, and vulnerabilities in the critical information systems could be exploited by adversaries. They seek to incapacitate critical infrastructure and key resources to threaten national security, causing considerable mass casualties, weaken world economy, and damage public morale and confidence. Cyberspace is far from secure today. In the light of this changing environment, there is an urgent need to take action – at national as well as international levels – against all forms of cybercrime.

During the last years, the Arab countries have achieved successful developments in the areas of information and communication technology and how individual, business and governments variables in assessing the current state of development and the impact of national and regional ICT strategies. For instance, Arab States are displaying significant interest in technology initiatives and are increasing their benefits like creating opportunities for research and development, developing technology diffusion and benefiting the social and economic environment by creating new employment possibilities.

Due to this radical change, Arab countries representatives recognized the need to foster throughout national and regional strategies, Cybersecurity related activities in order to better respond to cyber-attacks. Although Arab states have ICTs promotion and measures to undertake in order to safely use technologies, their approaches are often competing and fragmented. Thus, coordination and harmonization in terms of actions and legislative frameworks are required in order to have a unique position and being ready to defend cyber-attacks within the region.

2. PURPOSE OF THIS PAPER

Arab States are facing several challenges in addressing cyber threats and implementing appropriate legislative frameworks and national infrastructures to effectively combat cyber threats. The paper identifies several challenges that Arab nations face in order to enhance cybersecurity and at the same time secure the right infrastructure for protection of critical data. The document is aimed at assessing the measures taken by participating countries in confronting cybercrime threats. Finally, the paper concludes with a set of actionable recommendations for development partners and governments to undertake, including implementation of comprehensive capacity building programs, encouraging the implementation of national computer emergency response teams and coordination at the regional level.

3. SUMMARY OF THE EXISTING SITUATION

Member States of the Arab League presents a multifaceted situation in terms of existing legislations concerning cybercrime, implementation of national centres dealing with security problems with the ability to respond to major incidents and active measures to protect children online.

3.1 National and regional regulatory policies and frameworks for data privacy and fight cybercrimes

Most governments relatively recently have drafted national frameworks which address the issue of cybercrime. The problem is that these legislative prescriptions concern specific cyber threats and are mostly linked to e-commerce while unfortunately in recent years, cyber threats span over several domains, besides e-commerce, and a holistic approach is required to fight them.

Other countries need to start from developing substantive law and coordinating with national agencies working with security and cyber related activities. In some of them, there is no comprehensive cybersecurity law enacted or adopted yet. ICT related crimes are usually treated with the existing penal codes, thus many times they are not updated or aligned to global trends. A legislative vacuum has emerged in the field of ICT related crimes and offences, making it inevitable for the legislator to intervene in order to promulgate national legislations which include legal texts that guarantee the criminalization of activities resulting from the new technology in light of the traditional texts which have become inadequate to apply in the field of ICT. As noted, according to international standards, legislation should cover areas such as (i) criminalization, (ii) procedural measures, (iii) electronic evidence, (iv) jurisdiction, (v) liability of ISPs, and (vi) international cooperation.

In the Arab countries, regional cooperation is critical to fight these crimes, as they originate from different locations with modern techniques. The Arab region desperately needs to consolidate regional cooperation mechanisms to fight these types of crime already spreading in the region, under the absence of any special laws to counter them. Nonetheless, serious efforts are deployed to adopt a special convention on Arab regional cooperation to fight computer-related crimes or cybercrimes, which so far is still a mere attempt; furthermore, an Arab Guiding Law on Combating Information Technology Crimes was also adopted.

Lastly, incorporation of international standards is important in national legal systems (some countries may say that existing offences are adequate) to facilitate international cooperation (such that all countries operate with similar offence elements) and avoid the de facto evolution of legal 'safe havens' within the region.

3.2 Establishment of national Computer Security Incident Response Team (CSIRTs)/Computer Emergency Response Team (CERTs) and their coordination

Unfortunately, just few of Arab States members of the League of Arab States have implemented national centres for fighting cyber-attacks. As a consequence, it is difficult to respond efficiently to a

cyber-attack and resolve it. In this regard, assistance needs to be provided and coordination among Arab member states has to be put in place.

In particular 8 of the 22 countries (such as Oman, Saudi Arabia, and Tunisia) have implemented national CERTs and not all of them are coordinating with each other at the regional level. For some countries such as Egypt, Morocco, and Qatar, the establishment of the CERT has been a priority on the agenda of the government so that they created a holistic approach to achieve cybersecurity from the legislative, capacity building and infrastructure point of view. For other countries in the region, instead, it is still something that needs to be done after setting up legislative and regulatory framework; thus the implementation of Computer Emergency Response Team is still awaited or coming together slowly.

Through two big important regional initiatives, some countries who have already established national CERTs have decided to coordinate themselves with the aim of building a safe cyber space that provides convenience and peace to their citizens. For instance, the Cooperation Council for the Arab States of the Gulf- Computer Emergency Response Team (GCC-CERT)¹ is regional cooperation amongst Gulf States (Oman, UAE, Qatar, Kuwait, Saudi Arabia and Bahrain) on the topic of information security. The aim is to share views, best practices and give recommendations on the issues related to the cyberspace.

Moreover, acknowledging the threats in the cyber world, the Organization of Islamic Cooperation (OIC) has agreed to the establishment of inter Computer Security and Incident Response Team (CSIRT) or the Computer Emergency Response Team (CERT) collaboration among its member countries. Presently, 18 OIC countries are members of this collaboration and various activities are being conducted with the main objective being to facilitate the development of CSIRT capabilities, information sharing on views and issues in Cybersecurity. OIC-CERT has also established numerous collaborative initiatives and partnerships with regional CERTS, in order to strengthen Cybersecurity of the region.

3.3 Protection of Arab children and youth from harmful content on the Internet

Some Arab countries have actively addressed the issues of protecting children online and started activities to promote online safety at the national level. These countries have set up an inter-institutional committee or working group, composed of different stakeholder groups: government, industry, the legal profession; relevant NGOs; child welfare organisations; academia, to ensure implementation of the national child online protection strategy. In some countries, their national CERTs take the leading role to carry out the national strategy to promote the culture of ICTs security in the society, introduce Internet safety standards, raise awareness about the ethics of propose use of ICTs for children, and so on.

Some other countries in the region, however, still need to develop their national strategies on child online protection, such as proactive measures, common standards, legislation or raising awareness. In particular, it is necessary to have regional and international cooperation to exchange experience and improve ways of protecting children on the Internet.

4. CHALLENGES AND OPPORTUNITIES

The member states of the League of Arab States face several challenges related to different aspects such as legislative environment, user awareness, and national infrastructure.

As a counterpart of the positive effect of the ICTs, private sectors, international organizations together with governments are offering solutions and global responses to international cyber threats. However, at

¹ <http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/lewis-Q-CERT-incident-management-brisbane-july-08.pdf>

the national level, countries are required to improve national capabilities (human resources, infrastructures, legislative framework) to be better prepared to deal with cybercrimes.

- ICTs sectors need a proactive and encouraging global market in which to grow. This requires the existence of a reliable legislative framework able to regulate and if needed effectively deal with violations of the misuse of ICTs as well as a holistic approach involving cooperation between the private sector and government, awareness raising and prevention activities. Governments, private sector and NGOs need to coordinate their efforts and work together on the establishment of this framework. Most developed countries, as well as some developing countries have already updated their legal and regulatory frameworks in line with the needs created by the adoption of new technologies, however, the development of regional directives that promote the harmonization of ICT legislation and regulations sets the foundation of an enabling environment by facilitating and accelerating the use of ICT applications. In this regard, most Arab countries have set up a regulatory framework which does not necessarily fight global cyber threats nor is it harmonized regionally.
- The heavy investment made in recent years by the Arab nations in the fields of research, education and ICTs speak of their commitment to transition to a knowledge-based economy. An economy that depends on the deployment and pervasive use of ICTs, requires by default both knowledge and confidence in the use of ICTs. This assumes the twin capacity building needs – knowledge/capacity to use and the medium term capacity to deploy/innovate/indigenize - and finally the long term transition to the culture of ease and confidence. However, Arab states are not sufficiently investing on building capacity to raise awareness on cyber threats through educational programs – i.e. measuring the use, impact and threat of applying ICTs-, as well as to facilitate and promote internet safety tools and actions.
- While some Arab states have cybersecurity programs included in their national plans, this does not necessary mean that they are investing in creating national infrastructure able to help governmental authorities or local people respond to cyber threats. Few investment plans aim at financing the creation and growth of strategic components of the national infrastructure. For this, financial mechanisms aimed at ensuring investment for the security in the cyberspace have to be defined and adopted in the transition from the traditional reactive stance to an incrementally proactive stance.

The complexity of the challenges require cross-cutting approaches in the form of multi-stakeholder processes on the one hand and enhanced inter-service co-operation between the various authorities concerned on the other.

Through the League of Arab States it could be relevant to have a harmonized approach of Arab Member States in terms of legislation and financial investment for a safer cyberspace and create a regional cyber defense strategy to fight cybercrimes. Moreover, having in common cultural and religious aspects, Arab States are in the position to establish at the regional level mechanisms such as deployment of educational programs, engagement of private sector, and cooperation with local organizations. Some of the existing regional initiatives such as OIC-CERT or GCC-CERT could help to stimulate the establishment of other national CERTs and their coordination.

5. CONCLUSIONS AND RECOMMENDATIONS

On the basis of what has been highlighted in this report, and within the goal of Connecting Arab States, there is a need to quickly take actions for those countries that do not present any national strategy oriented to build up a cybersecurity infrastructure. For countries that already have an advanced structure both at the national and regional level, there is a need to strengthen cooperation and collaboration to create a harmonized regional strategy on cybersecurity.

5.1 Legislative Framework and Organization Structures:

1. The decision makers at governmental and ministerial levels need to take into account and allocate sufficient priority to security, reliability and availability of systems in all ongoing ICT infrastructure

projects. Principle of defense in depth should also be adopted by the governments in all the projects related to ICT.

2. Stakeholders should expedite the process of amending or passing of cyber laws in order to ensure that legal frameworks are consistent with cross-national standards in the areas of criminalization, procedural measures, electronic evidence, jurisdiction, and liability of ISPs. Such legal framework should be able to address not only national issues, but facilitate international cooperation as well.
3. Member States of the League of Arab States should seek technical assistance where required in order to expedite the processing of in-depth legislation review and amendment where necessary.
4. It is important to develop and implement awareness campaigns to educate users, law enforcement and policy makers about cyber laws, the impact of cybercrime and measures of combating it. The National CSIRT/CERTs can take on the leading role of creating Cybersecurity awareness campaigns.
5. The policy makers should raise awareness about the risks of technological progress for the market and consumers and consider regulatory measures to address issues such as personal and data protection, protection of minors, protection of end-users from the malware.
6. One of the most pressing things at the moment is the establishment of the National CSIRT/CERT and getting the technical expertise to operate it. To this end the experience acquired by Arab member states who have established their own CSIRT/CERT in addition to the experience of the ITU in assisting Member States can be made available.²
7. To impart the culture of cybersecurity, stakeholders can also embark on activities such as research programs relevant to Cybersecurity areas with tertiary students. The research programs can be coupled with rewards such as scholarship or employment to encourage more participation.

5.2 Capacity building:

The implications of building a culture on Cybersecurity are several and crosscut all sectors: security strategies & policies, legal framework & regulations, systems & processes, technologies & tools, skills & awareness, cooperation & networks. And as effective change management recommends, a pervasive change like this is to be accompanied by an all-encompassing strategy to facilitate human and institutional capacity building, which essentially would comprise of a programme of awareness building, education and training for the building of appropriate skill sets to gradually transition to the 'new' culture. Some of the aspects include:

1. The program of awareness building for the entire relevant population with targeted messages through broadcast methods.
 2. Use of computer technology and ICTs at all levels of formal education.
 3. A generic cyber-security education curriculum at higher education institutes.
 4. Specific curricula developed separately for policy makers, legal department, police departments, accompanied by a targeted capacity building implementation plan with best practices, tools/ labs and workshops.
 5. Research institutions encouraged to study this subject through special grants and award schemes
 6. Local/regional universities and research institutes select external specialist institutes as partners or as mentoring /interning opportunity
 7. Strengthening of regional forums/bodies for the exchange and sharing of information, incidences, good practices and experience.
-

8. Develop guidelines, planning tools & manuals on Cybersecurity technology / policy aspects.
9. Develop Local Cybersecurity toolkits for policy-makers and other relevant sectors.
10. Develop training materials on technology strategies & technology evolution for the implementation of Cybersecurity.
11. Organize workshops, meetings and seminars to address technical, policy, legal and strategy issues for Cybersecurity
12. Provide assistance in developing laws & model legislation for Cybersecurity prevention
13. Identify Cybersecurity requirements and propose solutions for the development of secure ICT applications.
14. Assist in raising awareness and identify key issues to support a culture of Cybersecurity, and recommend models of good practice to support ICT applications and minimize Cyberthreats
15. Develop tools to facilitate information sharing on technology and policy issues, and on best practices relating to Cybersecurity.

5.3 Invest more on public awareness and education:

1. Development of global strategies to facilitate human and institutional capacity building
2. Training for criminal justice professionals
3. Encourage the private sector to report any information they might obtain concerning cybercrime to the appropriate law enforcement or social service authority.

5.4 Protect Children Online:

In addition, the very nature of the Internet means that there are no borders and successful online safety will recognize this and harness the best from around the world. Effective online protection strategies will learn from the successes and mistakes of others, especially neighbor countries in the Arab region, and will keep a watchful eye on global development and emerging trends. On these bases, below are recommendations which discussed and agreed at the ITU Regional Workshop on *Policy Advocacy & Capacity Building in Child Online Protection for the Arab Region*, held in Muscat, Oman on 30-31 October, to consider in the national framework for the Arab countries to protect children online.

1. To encourage all Arab countries to support the ITU initiative on Child Online Protection (COP).
2. To unify and coordinate all the awareness efforts for the Child Online Protection (COP) in the region.
3. To establish an "Arab Child Portal" as a project funded by ITU and the League of Arab States and to post it on the website of the Pan Arab Observatory for Safety and Cybersecurity.
4. To encourage the Arab countries to set up policies and strategies that would protect children in cyberspace and promote their safer access.
5. To share best practices in particular the experience of Bahrain and to sign a MoU with the TRA in Bahrain regarding the use of their experience for the benefit of other countries.
6. To promote regional/international cooperation and to unify the efforts for sharing advice and information.
7. To encourage the Arab countries to set up legal procedures for promoting and supporting local manufacturers for creating special software and Arabic content for the Child Online Protection.
8. To set up mechanisms to promote the partnership between Governments and the software manufacturers to provide the safer solutions for Child Online Protection.

9. To find a way to obligate the internet cafes in all the Arab countries to use the Minors Web Browsers for the child online protection.
-

ANNEX

Summit Objectives and means (as identified by the Working Group on Trust and security)

Objectives

1. Establish a pan-arab agreement on cybersecurity and cybercrime, harmonized with existing international norms and principles, and in support to global cooperation on the topics
2. Development of a national cybersecurity strategies, aligned with international cooperation principles, including Critical Information Infrastructures Protection (CIIP), within the period of 5 years
3. Establishment of national legal frameworks harmonized at the regional level in all Arab countries, within the period of 5 years
4. Establish cybersecurity related curriculum aimed at building capacity and raise awareness in the various constituencies (e.g. Governments, Academia, Private Sector, Schools).
5. Establishment of Computer Security Incident Response Teams (CSIRTs)/ Computer Emergency Response Team (CERTs), in the Arab countries that do not have it, within the period of 3 years
6. Emphasize the importance of Child Online Protection (COP) and safety of children and youth, through awareness programs and establishment of technical measures

Means

1. Play an active role in discussions and activities related to internet international public policies
2. Establish an expert working group, with clear ToR and responsibilities, aimed at:
 - a. Undertake a thorough analysis in the region (in a form of a study) aimed at identifying gaps and elaborate a roadmap to implement the identified Objectives and actions to bridge the gaps
 - b. Instigate the process of know-how transfer and information sharing among the Arab Countries, making use of regional and national best practices as well as success stories, to better assist countries in need
3. Encourage investments and Private Public Partnerships