Cybersecurity and capacity building in the Arab region

The need for cyber security is magnified by the level of digitization and technical penetration that the Arab region is experiencing. For instance, the Internet penetration rate is generally higher than 90% and, in some cases such as Kuwait, UAE, and Qatar, approaches 100%. As such, many Arab countries have recognized that the security of cyberspace is an integral part of their economic systems and a matter of national security. This awareness has been followed by policies and actions: In the International Telecommunication Union's (ITU) Global Cybersecurity Index the states of Oman, KSA, Egypt, UAE and Qatar rank among the top-20 countries globally—with a considerable part of the Arab countries consistently ranking higher than many European countries. The strive for cyber security is a global as much as a local—and also Arab—endeavor, and the Arab region is gaining pace in cyber security research efforts and achievements.

Cyber security can be considered as specific to the Arab region as computing itself: Many of the threats, software and hardware developments, and industrial endeavors relating to cyber security are not exclusively tied to the region but are instead of a global character due to the nature of digitalization.

However, the political, economic, cultural, and financial contexts of Arab countries create a particular environment for facing attacks and addressing cyber security issues. The way the Arab world responds to cyber security challenges—in a broad but common understanding encompassing also trust and privacy—does not happen without tension or regional specificity: for instance, the protection of families and the respect for family life are an integral part of the Arab culture, while the strive for privacy protection is neither rooted nor strongly manifested in everyday digital life in Arab countries. Furthermore, while certain Arab countries are well known for their strong financial standing and politically stable systems—some being at the forefront of creating digital societies—others are suffering from war, instability, corruption, and poverty, which creates a heterogeneous and fragmented environment for threats and defenses on various scales.

Consequently, awareness of the importance of cyber security raised within the national governments in the Arab region, and has been recognized by national governments. One testimony of Arab research efforts in cyber security are the creation of academic research centers. One can observe committed endeavors toward the creation of secure digital environments within Arab countries, manifested by the development of national cyber security strategies and the establishment of national cyber security agencies—at varying levels of maturity and scope. National cyber security strategies exist or are in rollout for several Arab countries while others have occurred as drafts or are in development. For other Arab countries, the recognition of cyber security as a matter requiring a national
strategy is gaining momentum. The endeavors have been well directed and managed, as shown by international benchmarks. For instance, ITU's cybersecurity index is overall rising in many Arab countries, indicating the national strategies, capabilities, and programs in the field of cyber security are on the rise.

Oman hosts the Cybersecurity Innovation center for the Arab Region which has been launched in March 2013. The center aims to create activities that helps in enhancing regional cooperation, coordination and collaboration to address increasing cyber threats as well as sharing Information through best practices.

The ITU Regional Cybersecurity Centre (RCC) is a physical center hosted by Oman to act as the regional focal point for cybersecurity issues as well as deliver cybersecurity services to all partner countries within the agreed regional scope, with the following main objectives:

- strengthen the regional cybersecurity posture and increase the number of cybersecurity initiatives and projects within the region;
- localize ITU’s cybersecurity services to better fit the regional needs and requirements as well as language and cultural requirements;
- build and strengthen regional collaboration in cybersecurity issues;
- construct a global network of Regional Cybersecurity Centers that will assist in building a truly global cooperation on cybersecurity issues and contribute to the global culture of cybersecurity.

LAS in cooperation with the ITU assists in improving cybersecurity capacity development and incident response capabilities of countries by conducting cyberDrills for the Arab region. The ITU regional cyberDrills are designed with a dual purpose: as a platform for cooperation, information sharing, and discussions on current cybersecurity issues, as well as to provide hands-on exercise for national and regional development.

The regional cyberDrills are annual events which serve the purpose of:
- Enhancing cybersecurity capacity and capabilities through regional collaborations and cooperation.
- Enhancing the awareness and the capability of countries to participate and to contribute to the development and deployment of a strategy for defeating cyberthreats.
- Strengthening international cooperation between Member States to ensure continued collective efforts against cyberthreats;
- Enhancing Member States’ incident response capabilities and communication.
- Assisting Member States to develop and implement operational procedures to respond better to various cyber incidents, identify improvements for future planning and CIRT processes and operational procedures.
In Nov 2022 LAS in collaboration with the ITU and ARCC plan to organize a regional drill, and also provide many of Cybersecurity Trainings on the ITU Academy platform – Delivered by the Centre of Excellence in collaboration with the League of Arab States in areas of cybersecurity fundamentals, Forensic Programming and Ransomware Analysis.

Despite the efforts and results described here, Arab countries continue to be popular targets for cybercriminals, partially due to their financial power and oil resources, but also due to their location in a region full of geopolitical tensions. With the transition to new ways of engaging into conflict, cyber security is essential in the modern cyber-defense landscape.

Maintaining the security of information and communication technology (ICT) networks needs close collaboration between governments and industry. And because attacks do not respect national borders, efforts are required on an international scale.

The role of the private sector and that of governments in leading national cybersecurity efforts was discussed before, with participants stressing the need to review national laws to ensure that they address threats in cyberspace.

Every national government in the region is striving to create a secure digital environment, but too often these efforts are fragmented, tactical, and reactive. Moreover, they do not include the participation of all essential stakeholders. Consequently, governmental responses often lag behind the ever-evolving threat landscape, and the defensive measures taken are circumvented or exploited. A strategic approach to national cyber security is needed that follows a “CCC” framework — comprehensive in nature, collaborative by intention, and capability-driven.

Arab governments can apply the GCC framework in their own national cybersecurity programs. First, they should establish a centralized national cyber-security body, with a clearly defined mandate. The established body should define a national cyber-security strategy and establish the national dialogue. Afterwards, there should be a focus on building cyber-security capabilities, both preventive and reactive, and on developing the talent and capabilities on which national cyber security rests. By acting immediately on these imperatives, governments will ensure that their nations reap the full rewards of digitization, now and in the future.

They are acutely aware of the new threat landscape associated with digitization. To support their national cyber-security capabilities and elevate the protection level of their critical national information infrastructures, many of them have stepped up their cyber-security activities in recent years.

Some countries have created new laws aimed at protecting electronic transactions and prosecuting cyber-crimes. Others have established critical
information infrastructure protection polices and cyber-security plans, and have vested responsibility for cyber security in existing agencies or directorates. Still others have initiated national incident response protocols, and have begun building cyber-security awareness and capabilities. These are all good steps toward improving national cyber security. However, these steps alone will not suffice to manage risks associated with the digital assets of an entire country.

Most of these existing initiatives take an IT-centric approach to national cyber security. They are tactical responses to an issue that requires a strategic solution. A national cyber-security program requires a coherent, comprehensive strategy that identifies essential national cyber capabilities, and clearly assigns ownership of these capabilities and responsibility for national cyber security to a dedicated lead agency.

**To conclude:** The governments of the Arab world are the only stakeholders with the power, reach, and resources necessary to develop and drive a truly national cyber-security agenda, to ensure alignment of efforts, and to drive collaboration and continuous improvements through sector-specific, national, and ultimately regional governance bodies. This is why it falls to government to define a national cyber-security program, assign ownership and responsibility at the highest level, and launch the program. All that remains is for Arab leaders to address this critical problem, which threatens their national digitization efforts and prospects for viable, twenty-first century economies.

- Recently there is a coordinating body consists of the technical secretariats of Arab interior ministers, justice ministers and telecommunications and information technology Arab ministers so as to coordinate between them to propose capacity building programs that can serve all the Arab region so as to avoid duplication.

- The Arab information and Communication Technology launched the Arab strategic vision for cyber security in October 2021 which will be an input for the Arab telecommunication and information technology Strategy that will be finalized at the end of the year 2022.

- The League of Arab States is working with related regional and international organizations to help least developed Arab countries concerning cyber security capacity building.