Regional Intergovernmental Organizations

While large international organizations such as the United Nations and OECD are currently pursuing global cyber security initiatives, a large amount of work is also being done by smaller, regional intergovernmental organizations. Regional organizations have the potential to make an impact because of their ability to relate to the needs of their smaller constituencies. However, because regional organizations frequently lack the funding and full support of member states, it is often a challenge to garner enough cooperation to make any recognizable impact on the global scale.

A majority of initiatives by regional intergovernmental organizations, aside from the work done by the Council of Europe on the Convention on Cybercrime, have been limited to providing resources to their member states and opening communication channels between nations. Cyber security policies and initiatives are in different forms and stages of implementation in different parts of the world. For example, the European region, with organizations such as the European Union, leads the way with regard to initiative success. Other organizations, such as APEC and the Organization of American States (OAS), are making similar progress in other regions around the world, such as Asia-Pacific and the Americas.

Although regional intergovernmental organizations in Africa and the Middle East have recently begun to show a greater interest in developing cyber security policy frameworks, training and awareness programs, and incident response capabilities, many of these activities still appear to be in a very early stage of development. Because many of the primary organizations with ICT security objectives in the Middle East, such as the League of Arab States and the Gulf Cooperation Council, do not offer extensive Arabic-English translation on their websites, these organizations have not been included in this section.

The following subsections include a breakdown of regional organizations currently active in the cyber security arena in Europe, Asia-Pacific, and the Americas, including a brief discussion on noteworthy activities dealing with intergovernmental policy implementation, harmonization of legal frameworks, cybercrime awareness, incident response, and law enforcement. Detailed analysis on the present state of cyber security in Africa is currently available in a separate ongoing study at Georgia Tech, accessible from the online Cyber Security Organization Catalog.
4.1 Europe

4.1.1 European Union (EU)

Established in 1993, the European Union is the largest governing body within Europe. The EU represents twenty-seven European countries and was established around three pillars: the European Communities, common foreign and security policy, and police and judicial cooperation in criminal manners. In particular, the third pillar has enabled the European Union, through a series of Directives and Communications by the Commission of the European Communities (“the Commission”), to play a very active role in developing policy initiatives to combat cybercrime and promote a regional culture of cyber security in Europe since the 1990s.

The Information Society and Media Directorate General “supports the development and use of Information and Communication Technologies (ICTs) for the benefit of all citizens.” Its role is to: “Support innovation and competitiveness in Europe through excellence in ICT research and development; define and implement a regulatory environment that enables rapid development of services based on information, communication and audio-visual technologies, so fostering competition that supports investment, growth and jobs; encourage the widespread availability and accessibility of ICT-based services, especially those that have the greatest impact on the quality of life of the citizens; foster the growth of content industries drawing on Europe’s cultural diversity; and represent the European Commission in international dialogue and negotiations in these fields, and promote international cooperation in ICT research and development.”

Three committees of the European Parliament focus on the Information Society: The Committee on Industry, Research and Energy (ITRE); the Committee on Civil Liberties, Justice and Home Affairs (LIBE); and the Committee on Culture and Education (CULT). ITRE is responsible for “the information society and information technology, including the establishment and development of trans-European networks in the telecommunication infrastructure sector.” Specific to information security, LIBE is responsible for “legislation in the areas of transparency and the protection of natural persons with regard to the processing of personal data.” CULT is responsible for the “audiovisual policy and the cultural and educational aspects of the information society.”

In March 1992, the European Council approved its first initial action in the field of security of information systems, establishing an action plan and a Senior Officials Committee. In an early attempt to assess the landscape of cyber security in Europe, the Commission presented the results of a study on computer-