Group of Governmental Experts (GGE)

Geneva, 12 – 16 January 2015

SamehAboul-Enein (Egypt)

Themes and Concepts for Cyber Security Development

1. The political transition in the region has undoubtedly changed fundamental dynamics in the Middle East, with significant implications for role of information technology, as an integral part of the future of security architecture in the Middle East.
2. Public opinion increasingly plays a more prominent role in Arab societies and communications technologies provide a notable platform to transfer this public opinion to the decision-making institutions faster and more representatively. Therefore, many States in the region give high consideration for developing its cyber infrastructure and exert all possible efforts to update their cyber security techniques and capabilities.
3. Cyber Security could be considered as an emerging challenge that interlinks with other political challenges in the region, such as the critical socio-economic challenges, the regional and cross-national terrorism, the proliferation of conventional weapons and small arms and light weapons, and education, awareness and capacity-building.
4. In addition, cyber security is crucial for maintaining nuclear security. The NSS in the Hague in March 2014 recognized the growing importance of information security, including information held on computer systems, related to nuclear material and technology. In these areas, cooperation between government, industry and academia is desirable.
5. On a practical note, there are a lot of measures that States should take in order to promote measures of restraint in cyber armaments; in their use of ICTs, States must observe their obligations under Article 2 of the United Nations Charter to settle international disputes by peaceful means, as well as the prohibition of the threat or use of force. In the context of ICT Security, threat or use of force would also encompass the destruction or causing harm in any form to all layers of the ICT infrastructure, whether physical or digital, of a Member State.
6. I specify in particular three interlinked layers of the challenges to cyber security buildup: a) telecommunications and related infrastructure; content and ICT related applications, and content and its related applications. In this regard, more efforts geared for developing and implementing confidence building measures to diffuse cyber tensions and to mitigate cyber risks are needed.
7. Gaps in capacity related to ICT security among States, especially with the rapid increase in vulnerabilities across in an interconnected world, and expanding challenges to developing countries due to the limited resources. Developing countries are most affected by the negative impact of adverse and malicious uses of ICT, commensurate capacity building and adequate transfer of knowledge and technology should be integral to any multilateral initiatives regarding ICT security.

8. In this regard, there are two issues to be highlighted here:

i. Focus on the effective implication of the recommendation that "capacity building is of vital importance to an effective cooperative global effort on securing ICTs and their use." There should be more efforts to provide assistance to the States in order to "improve the security of critical ICT infrastructure; develop technical skill and appropriate legislation, strategies and regulatory frameworks to fulfill their responsibilities; and bridge the divide in the security of ICTs and their use".

ii. Development of training programs to help overcome the digital divide and help developing countries cope with international developments in the field of public policy, and to consider ways in which the United Nations Institute for Training and Research, along with other international and regional centers and organization can play in this regard. Also, there should be more regional and international cooperation and coordination through creating and strengthening incident response capabilities, including CERTs, and strengthening CERT-to-CERT cooperation

9. The development of training programs to help overcome the digital divide and help developing countries cope with international developments in the field of public policy, and to consider ways in which international and regional centers and organization can play in this regard. Also, there should be more regional and international cooperation and coordination through creating and strengthening incident response capabilities.

10. It is important to highlight that the legislative framework to reinforce the cyber security regimes on the national level is still under development in the different states of the region, specially in a challenging security environment, where many non-state actors are conducting terrorist attacks through cyber-warfare techniques.

11. In Conclusion, it is important to highlight that cyber warfare has several forms, and there are multiple techniques and mechanisms on how cyber attacks may affect civilian devices, services and applications. Therefore, cyber security cooperation remains a part and parcel of any regional or international security arrangements.