Cooperation in addressing Cyber Security Challenges

Dr. Sameh Aboul-Enein

Professor of International Security and Diplomacy

(The Geneva Center for Security Policy, The Geneva School of Diplomacy and International Relations, and The American University in Cairo)

NATO Regional Cooperation Course
April 12th 2016
# Table of Content

- **I. Cyber Technology**
- **II. The Emergence of Cyber Security as a Modern Threat**
  - a) Cyber Attacks and Cases
  - b) Challenges to Cyber Security Building
- **III. Cyber Security in the Middle East**
  - a) The Increasing Importance of Cyber Security in the Middle East
  - b) Computer Infections in ME
- **IV. Report of Group of Governmental Experts On Developments in Fields of Information and Telecommunications In the Context of International Security**
  - a) International Cooperation and Assistance in ICT Security
  - b) Recommendations for Future Work
- **V. Competence Building Measures**
- **VI. Concluding Remarks**
  - a) Security Dynamics in a Politically-Changing Region
  - b) Cyber Diplomacy
  - c) Measures to be Taken by States to Face Cyber Security Threats
  - d) Creation of a global culture of cyber security
I. Cyber Technology

- Cyberspace has become an essential component of modern society. Social infrastructure, the financial sector, government services, security, schools, and hospitals are irreversibly dependent on interconnectivity and the global network.

- In the last few years, cyber technology has developed substantially and will continue to grow; the more it provides ease and effectiveness in different aspects of societies, the more it will become embedded in societal and governments’ systems. However, the merits of the open internet are accompanied by several threats.

- The rapid evolution and the multidisciplinary nature of cyberspace has made it and urgent matter of study. A comprehensive approach for strategic foresight planning has become essential to secure societies from the growing number of potential cyber-threats.
II. The Emergence of Cyber Security as a Modern Threat

- The Field of Cyber Security is witnessing a growing importance in our modern world due to the reliance on computer systems in most societies.

- “Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards.”

  *US Department of Homeland Security*

- Failure of states to install adequate cyber security measures could result in putting all its industries, such as financial systems, government, and military at grave risk.
According to estimates by the Center for Strategic and International Studies, cyber crime costs the global economy over US$400 billion per year.

The Global Risks 2015 report, published by the World Economic Forum (WEF), included this rather stark warning: “90 percent of companies worldwide recognize they are insufficiently prepared to protect themselves against [cyber attacks].”

Cyberspace is particularly difficult to secure due to:

- The ability of malicious actors to operate from anywhere in the world,
- The linkages between cyberspace and physical systems
- The difficulty of reducing vulnerabilities and consequences in complex cyber networks.
The strategic imperatives of national cyber security

1. Comprehensive
   Identify and engage all aspects and players of the cyber-security ecosystem

2. Collaborative
   Ensure that digital asset protection is a shared responsibility of the private sector, public sector, and citizens

3. Capability-Driven
   Build both reactive capabilities and proactive capabilities that enable the prevention and deterrence of cyber attacks
a) Cyber Attacks and Cases
Examples of Cyber Attacks

- **Stuxnet**
  - In 2010, The Stuxnet software worm repeatedly sought to infect five industrial facilities in Iran over a 10-month period, in what could be a clue into how it might have infected the Iranian uranium enrichment complex at Natanz.

- Symantec, a computer security software firm, said there were three waves of attacks that the worm took aim at in specific organizations in Iran between June 2009 and May 2010. “Stuxnet recorded information on the location and type of each computer it infected”. 
Examples of Cyber Attacks (cont.)

- **Saudi Aramco Cyber Attacks**
  - In 2012, a group named "Cutting Sword of Justice" claimed responsibility for an attack on 30,000 Saudi Aramco workstations, causing the company to spend a week restoring their services. The group later indicated that the Shamoon virus had been used in the attack.

- Former NSA boss Gen. Keith Alexander has claimed that the Shamoon malware attacks on Middle East energy company Saudi Aramco in 2012 were a “wake-up call for everybody” that could have severe repercussions for the safety of critical infrastructure networks.
ISIS and Cyber security

- The dangers posed by Isis may be more dangerous than any other terrorist group because of its embrace of modern technology, mastery of the difficult art of online propaganda and its appeal to young, computer-literate foreigners, including known hackers.

- In January 2015, the Twitter and YouTube accounts of the US Central Military Command (Centcom) were hacked by a group calling itself the “CyberCaliphate”. The hackers scrawled, “I love you Isis”, across the page and sent out tweets including pictures showing US personnel in a command outpost and military documents, suggesting Isis sympathizers had somehow infiltrated military servers and installations.
b) Challenges to Cyber Security Building

- I specify in particular three interlinked layers of the challenges to cyber security buildup:
  - Telecommunications and related infrastructure.
  - Content and ICT related applications.
  - 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.
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.
III. Cyber Security in the Middle East

- The continuing success of digitization initiatives among the countries of the Middle East brings with it an added and growing exposure to the risk of cyber attacks. These attacks — by other states and by increasingly sophisticated criminal rings from around the world — have the potential to derail the progress of digitization, and threaten the benefits delivered through it.

- 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.
The serious challenge that Cyber Security has become; interlinks with other political challenges, such as regional and cross-national terrorism. In this respect, efforts and demand-driven programs should be invested to help local governments create suitable environment for sustainable socio-economic conditions to overcome the roots of poverty and terrorism.

It is important here 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. Many States give high consideration for developing its cyber infrastructure and exert all possible efforts to update their cyber security techniques and capabilities.
a) The Increasing Importance of Cyber Security in the Middle East

- 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.

- 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.
• Nation states have developed unparalleled cyber exploitation and attack technologies that they are beginning to integrate into their national military capabilities.

• Middle East countries are pursuing digitization — the mass adoption of connected digital technologies and applications by consumers, enterprises, and governments — at a rapid pace. The region’s digital markets are expanding at an overall compound annual growth rate of 12 percent and were expected to be worth US$35 billion in 2015. Strategy& estimates that digitization could add as much as $820 billion to regional GDP and create 4.4 million new and much-needed jobs by 2020.
b) Computers become infected in the Middle East at increasingly higher rates than the global average
IV. Report of the Group of Governmental Experts On Developments in the Field of Information and Telecommunications In the Context of International Security
a) International Cooperation and Assistance in ICT Security and Capacity-Building

- States bear primary responsibility for national security and the safety of their citizens, including in the ICT environment, but some States may lack sufficient capacity to protect their ICT networks.

- The 2013 GGE Report called upon the international community to work together in providing assistance to improve the security of critical ICT infrastructure; develop technical skills and appropriate legislation, strategies and regulatory frameworks to fulfill their responsibilities; and bridge the divide in the security of ICTs and their use.

- The current Group also emphasized that capacity-building involves more than a transfer of knowledge and skills from developed to developing States, as all States can learn from each other about the threats they face and effective responses to them.
b) Recommendations for Future Work

- Recognizing that ICTs can be a driving force in accelerating progress towards development, the Group considered it useful to identify possible measures for future work, which include, but are not limited to, the following:
  - Further development by States collectively and individually of concepts for international peace and security in the use of ICTs at the legal, technical and policy levels
  - Increased cooperation at regional and multilateral levels to foster common understandings on the potential risks to international peace and the security posed by the malicious use of ICTs, and on the security of ICT-enabled critical infrastructure.
• While States have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations.

• Areas where further research and study could be useful include, inter alia, concepts relevant to State use of ICTs.

• The United Nations should play a leading role in promoting dialogue on the security of ICTs in their use by States, and developing common understandings on the application of international law and norms, rules and principles for responsible

• The Group noted the importance for the UN General Assembly to consider the convening of a new Group of Governmental Experts on Developments in the Field of Information and Telecommunications in 2016

• The Group acknowledges the valuable efforts in ICT security made by international organizations and regional groups.

• The Group recommends that Member States give active consideration to the recommendations contained in this Report on how to help build an open, secure, stable, accessible and peaceful ICT environment.
V. Competence Building Measures

- One of the most challenging issues facing cyberspace is developing qualified labor for the cyber security labor market.

- To tackle this challenge, there are eight steps that were identified to promote competence building. Those trends can be put under two categories:
  - Promoting cyber security competence building at universities
  - Promoting competence building through professional training
• Promoting cyber security competence building at universities:
  • Creating university programs supported by the government
  • Certifying and Labeling universities and study programs
  • Reaping the economic potentials (Investing in education)

• Competence building through professional training
  • State personnel training
  • Collaboration with professional certification bodies
  • Improving the competence of the private sector
  • Manager and decision-making level training
  • Knowledge frameworks, job descriptions, and professionalization of cyber security
VI. Concluding Remarks:

- 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.
a) Security Dynamics in a Politically-Changing Region

- 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.

- 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.
b) Cyber Diplomacy

- Cyber-diplomacy is the evolution of public diplomacy to include and use the new platforms of communication in the 21st century. It links the impact of innovations in communication and information technology to diplomacy.

- It recognizes that new communication technologies offer new opportunities to interact with a wider public by adopting a network approach and making the most of an increasingly multicentric global, interdependent system.

*Melissa Jan, The New Public Diplomacy*
Cyber Diplomacy complements traditional foreign policy tools with newly innovated and adapted instruments of statecraft that fully leverages the networks, technologies, and demographics of our interconnected world. It became a strategic block in capacity building, especially in the developing world, for the evolving diplomatic efforts towards the promotion and protection of human rights, rule of law, security, growth and development.

This puts a stress on the fact that cyber security is further from only being an issue to be tackled on a national levels, and that if compromised, cyberspace can have drastic effects on international and diplomatic relations as well.
c) Measures to be Taken by States to Face Cyber Security Threats

- 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.
d) Creation of a global culture of cyber security

- Assist in strengthening cooperative mechanisms with national CERTs and other authorized bodies
- Provide assistance and training to developing countries to improve security in the use of ICTs
- Assist in providing access to technologies deemed essential for ICT security
- Create procedures for mutual assistance in responding to incidents
- Facilitate cross-border cooperation
- Develop strategies for sustainability in ICT security capacity-building efforts
- Prioritize ICT security awareness and capacity building in national plans and budgets
- Encourage further work in capacity building
In this regard, there are two issues to be highlighted here:

- 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”.
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.

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.
For further readings and publications, please check:

http://www.gcsp.ch/About-Us-Qui-sommes-nous/Associate-Visiting-Fellows/Ambassador-Dr-Sameh-ABOUL-ENEIN

Thank You
On 4 December 2015, the NATO Defense College (NDC) celebrated the graduation of the 14th edition of the NATO Regional Cooperation Course (NRCC-14).

Upon arrival special guests to the ceremony were warmly welcomed by NDC Commandant MGen Janusz Bojarski (POL F), as well as by the Dean Dr Daria Daniels Skodnik (SVN C) and by the Director of the Middle East Faculty Col Giuseppe Morabito (ITA A).

Before Course Members received their graduation diplomas and the congratulations of the NDC leadership, MGen Bojarski spoke about the importance of this unique Course, highlighting its value in promoting dialogue amongst participants and improving common understanding. The Commandant underlined that cooperation, rather
than unilateral action, is the key to facing future challenges together. One of NATO's great strengths is its respect for this principle.

NRCC-14 Course Members and guests were then addressed by Ambassador Dr Sameh AboulEnein (EGY) on “Emerging Regional Challenges”. The speaker recognized the growing importance of information security and the urgent need to develop an international mechanism for fighting terrorism. He underlined that the major challenges in maintaining peace and security are best addressed by dialogue and cooperation among Allies and Partners, committed to identifying appropriate solutions. In order to prevent nuclear armament and proliferation in the Middle East H.E. Dr AboulEnein indicated three main priorities: dismantling and destroying existing or remaining nuclear weapons; using nuclear materials and facilities for peaceful purposes; and addressing the issue of verification, with clear recognition of the role to be played by the IAEA.

NRCC-14 brought together 42 participants from 17 NATO, Mediterranean Dialogue, Istanbul Cooperation Initiative, as well as Global Partner countries. During their ten weeks at the NDC, Course Members established a stimulating environment for discussion with the aim of increasing future international cooperation and finding solutions to current issues.

The first Course (NRCC-1) was held in 2009, with the objective of enhancing dialogue, mutual understanding and cooperation between NATO and its Partners. The goal of the NRCC is to inform military and civilian personnel from MD, ICI and NATO countries who are working in the Mediterranean Region and the Middle East, or in their respective agencies, on current and future security challenges affecting the region.

After the graduation ceremony, NRCC-14 Course Members presented the NDC with a Sports Afternoon volleyball cup, which the NRCC had won for the first time ever this year, as a token of gratitude.