Loughborough University

Academy of Diplomacy and International Governance

Simulation Exercise: UN Simulation Week on Science and Diplomacy, Week 9-15 of May, 2016

Instructor: Dr. Sameh Aboul Enein

http://www.lborolondon.ac.uk/study/institutes-programmes/academy-of-diplomacy-and-international-governance/people/

I. Simulation Session: Nuclear Weapons Free Zone in the Middle East

The Loughborough University in London, under the supervision of Ambassador Dr. Sameh Abould Enein, conducted a simulation for a UN special session on nuclear disarmament in the Middle East. The simulation involved students from the Master Program at various stages of their academic program. The participating students represented countries and organizations that are most concerned with the topic. Represented countries and organization included the US, Russia, China, Egypt, Iran, Israel, the IAEA, the CTBTO, and several other states and organizations that are usually present around the negotiations table whenever a Nuclear Weapons Free Zone in the Middle East is on the agenda.

During the simulation, the students had the opportunity to represent the foreign policy stance of their respective states and to engage with their counterparts in formulating a draft resolution that is aimed towards solving the issue at hand. Students were able to experience what its like to be part of an international conference, and to become familiar with the working atmosphere and procedures in UN sessions.

II. Dr. Sameh Statement on Science diplomacy & international policy

Let me begin by extending my thanks and deep appreciation to Loughborough University in London for inviting me here to participate in the Science Diplomacy and International Policy Symposium. It is a privilege to be speaking here at one of the leading institutions in this field, in front of many experts and young people who I am certain will be making significant contributions to the development of science diplomacy in years to come.

I am here today to shed light on one of the most fundamental issues that is shaping modern diplomacy and to explain why developments in information and communications technology (ICT) raise significant challenges relating to international security. I will begin by briefly outlining how innovations in science and technology have fundamentally changed diplomatic structures, before outlining the key challenges posed by cyber warfare for states in the modern, globalized world. Following this I will outline diplomatic tools that can be used to combat these challenges and how these developments have played a major role in the political diplomacy of the Middle East.

Cyberspace has become an essential component of modern society. Every aspect of developed social infrastructure from the financial sector to government services, security, schools, and hospitals are completely dependent on cyber technology. Their effectiveness is determined by their connectivity and their ability to communicate within global networks.

In the last few years, cyber technology has developed substantially and will continue to grow at an exponential rate. As it provides greater ease and effectiveness in different aspects of societies, it will become further embedded within societal and governmental systems.

Like every other aspect of human life, modern sciences are significantly reshaping the manner by which nations conduct their foreign and diplomatic relations. The use of ICT in conducting international relations, otherwise known as science diplomacy, has markedly affected diplomatic interactions in current times.

This is most visible in how public diplomacy and engagement has been transformed through the use of new platforms of communication in the 21st century.

Science diplomacy has linked the impact of innovations in communication and information technology to diplomacy, and 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 multi-centric global, interdependent world. An example of this change is that it is now commonplace to read about governments using social media websites as tools for public diplomacy. This has fundamentally changed the way in which public diplomacy is conducted, as social media offers a breadth of engagement with public audiences on such a scale not previously available to diplomats in the 20th Century.

Cyber technologies and science diplomacy also complement traditional foreign policy tools with newly innovated and adapted instruments of statecraft that make full use of the networks, technologies, and demographics of our interconnected world. They have become a strategic block in capacity building, especially in the developing world, for the evolving of diplomatic efforts towards the promotion and protection of human rights, the rule of law, security, and growth and development.

Cyber culture is evolving at a faster than the technologies in the field of Cyber security. This means that the private data, intellectual property, and resources of conventional civilian and military infrastructure can be compromised or damaged by the ever growing threat of cyber attacks, unforeseen security flaws, and the internal vulnerability of the internet. This emphasizes the importance of maintaining cyber security on a national level, as if compromised, there can be potentially disastrous effects on international and diplomatic relations.

The unresolved issues of Cyber Security create an imbalance between state security and human security. This is arguably most crucial in terms of maintaining nuclear security. The Nuclear Security Summit in Washington in March 2016 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, if not essential in the modern information age.

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 destroy or cause severe harm to all layers of a country's ICT infrastructure, whether physical or digital.

I specify in particular three interlinked layers of the challenges to cyber security buildup: 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.

There are several key gaps in capacity related to ICT security among states, which have been worsened by the rapid increase in vulnerabilities across the interconnected world and the expanding challenges to developing countries due to the limited resources. Developing countries in particular are most affected by the negative impact of adverse and malicious uses of ICT. What is needed is commensurate capacity building and adequate transfers of knowledge and technology supported by multilateral initiatives regarding ICT security.

There are two issues to be highlighted here that were recommended in the 2013 report of the Group of Governmental Experts (GGE) on Development in the Field of Information Telecommunications in the context of International Security for capacity building measures:

I. Recognize 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 skills 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 organizations can play in this regard. In addition, there should be more regional and international cooperation and coordination through creating and strengthening incident response capabilities, including Computer Emergency Readiness Teams (CERTs), and strengthening CERT-to-CERT cooperation.

There have been significant improvements with regards to establishing cooperation mechanisms between regional and international parties in promoting cyber security and science diplomacy. International organizations such as the International Telecommunication Union and the Organization of Economic Cooperation and Development, have had several initiatives to better address cyber threats and have created programs for competence and capacity building. However, there are still a lot of measures that need to be taken to minimize the risk and maximize the gains of the implementation of ICTs in modern diplomacy.

The Group of Governmental Experts (GGE) issued its report in June 2015 and it identified possible measures for future work, which include, but are not limited to, the following:

I. 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; and

II. 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.

The report also added that states should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs, and implement other cooperative measures to address such threats. Cooperation initiatives should be in a manner consistent with domestic and international law, with requests from other states in investigating ICT-related crime or use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory.

Communication technologies have also played a major role in the political transition in the Middle East. They have undoubtedly changed the fundamental dynamics of the region, with significant implications for role of information technology, as an integral part of the future of security architecture.

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 give high consideration for developing their cyber infrastructure and exert all possible efforts to update their cyber security techniques and capabilities.

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.

In this regard, fresh momentum was injected into ICT development plans in the Arab world. At the Connect Arab Summit in Doha, Qatar, in 2012, support was directed to regional initiatives on access to broadband networks, digital broadcasting, open-source software, Arab digital content, and cyber security. Follow-up meetings of this summit, organized jointly by ITU and the League of Arab States, looked at ways of furthering the implementation of these regional projects.

The League of Arab States, in collaboration with the United Nations Economic and Social Commission for Western Asia (UNESCWA), has been committed towards capacity building and the proliferation of cyber security knowledge and technology, with the objective being the creation of a resilient, up to date cyber security ecosystem, shortening response time, and increasing cooperation between countries.

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, especially in a challenging security environment, where many non-state actors are conducting terrorist attacks through cyber-warfare techniques. These circumstances require a relentless focus on coping with new challenges through international and regional dialogue and exchange on ICT security issues. This dialogue allows for nation states and international organizations to be engaged in the process of building an efficient, integrated, legal, and politically sustainable international cyber security system.

In conclusion Cyber warfare has several forms, and there are multiple techniques and mechanisms on how cyber attacks may affect civilian devices, services, applications, and ultimately civilians themselves. It is important to recognize that science diplomacy will perpetually change the way foreign policy establishments operate; therefore, cyber security cooperation remains a crucial aspect of any regional or international security arrangements.

III. HE Amb Sameh Aboul Enein Programme from 9 to 14 May 2016 at ADIG, London

Monday 9 May 18h00 – 21h00	**Diplomacy: Policy, Practice and Procedures 2 Module** • *Conference Negotiations* • *Defence Diplomacy*	**HE Amb Sameh Aboul Enein & Professor Nabil Ayad**
Tue 10 May 18h00 – 19h30	**Diplomacy: Policy, Practice and Procedures 2 Module** • *Diplomatic Practice: Daily Life in an Embassy*	**HE Amb Sameh Aboul Enein & Professor Nabil Ayad**
Wed 11 May 18h00 – 21h00	**Pre-Symposium Reception**	**At the American Embassy**
Thurs 12 May 09h00 – 17h00	**The Symposium (The Ambassador's Panel)**	**Lecture Theatre (Phase II – New Building)**
Thurs 12 May 19h30 – 22h30	**Post Symposium Dinner**	**Churchill Hotel in Marble Arch**
Friday 13 May 18h00 – 19h30	**Diplomacy: Policy, Practice and Procedures 2 Module** • *UN & International Institutions: Economic and Security Organisations GATT, WTO, NATO* • *Nuclear Freezone* • *Cyber Security and Challenges*	**HE Amb Sameh Aboul Enein & Professor Nabil Ayad**
Sat 14 May 10h00 – 13h00	**Diplomacy: Policy, Practice and Procedures 2 Module** • *The UN Simulation Exercise*	**HE Amb Sameh Aboul Enein & Professor Nabil Ayad + All Staff**