GENEVA SCHOOL OF DIPLOMACY
& INTERNATIONAL RELATIONS
UNIVERSITY INSTITUTE

Preparation Sheet for Simulation

Topic: Cyber Security Attacks

February 17th 2016, (14:00 – 15:30 / 15:45 – 17:15)

Simulation Model on Cyber Security Attacks

Three students should volunteer to chair. Meanwhile, the rest of the students will choose a side they want to support and contribute to during the debate session.

Students are expected to choose their roles on Monday 13th February by 17h, and provide their choices to the TA.

During the simulation, the students will be divided into three teams, one team is supporting National Scenarios to counter Cyber Security Attacks (National Team), the second team is supporting Regional Scenarios to counter Cyber Security Attacks (The Regional Team), and the third team is supporting International Scenarios to counter Cyber Security Attacks (International Team)

An opening statement introduces a team's position and offers important evidence.
A Rebuttal is a team's response to its opponent's arguments.
A Second statement is a team's chance to expand upon their ideas and evidence

Stage 1:

- *In this formal session, each chair will give the opening statement. The opening statement will represent the position of the team and offer important evidence*
- *Each chair will have 10 minutes for the opening statement.*

Stage 2:

- *The first rebuttal should be a response to the opponent's arguments and a chance to give counter arguments*
- *Each student will have 2 interventions in this stage to respond to other delegations, and each intervention should not exceed 5 minutes*

Stage 3:

- *The second statement is a team's chance to expand upon their ideas and evidence*

LEARNING OUTCOMES OF THE SIMULATION

- Practice in speaking in public
- Practice in the use of diplomatic language and the required protocol
- Importance of careful preparation before speaking and the accuracy of facts
- Need to keep diplomacy active, with no "closed doors"
- Practicing alternative scenarios to crisis and to develop the ability to address complex situation in UN environment
- Realization of the dangers of becoming locked into positions and of stating preconditions before the commencement of negotiation
- The use of "ice-breakers" and "shared experiences" when appropriate to build trust

Readings:

Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School" *International Studies Quarterly* Vol. 53, No. 4 (Dec., 2009), pp. 1155-1175

- Available at: http://www.jstor.org/stable/27735139

Rex Hughes, "A treaty for cyberspace", *International Affairs (Royal Institute of International Affairs 1944-)* Vol. 86, No. 2 (March 2010), pp. 523-541

- Available at: http://www.jstor.org/stable/40664079

Sean S. Costigan and Gustav Lindstrom "Policy and the Internet of Things", The Quarterly Journal

- Available at: https://connections-qj.org/system/files/15.2.01_costigan_lindstrom.pdf

Costigan, S., Lindstrom, G. and D. Puhl, "Hybrid Conflicts as an Emerging Security Challenge: Policy Considerations for International Security", Partnership for Peace Consortium Policy Brief.

- Available at: http://www.pfp-consortium.org/index.php/pfpc-products/policy-papers/item/95-hybrid-conflicts-as-emerging-security-challenge-policy-considerations-for-international-security
- Geneva Center for Security Policy: http://www.gcsp.ch/content/search?SearchText=cyber+security

  http://www.gcsp.ch/News-Knowledge/Experts/Fellows/Aboul-Enein-Amb.-Dr-Sameh-Aboul-Enein/Selected-publications
- United Nations Office for Disarmament Affairs: http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html

  https://www.un.org/disarmament/topics/informationsecurity/

Crisis Scenario:

A major cyber incident has just occurred; United Nations Secure Web Services were attacked. The target was the UN servers that manage logistical and communications support to the United Nations Supervision Mission in Syria (UNSMIS), halting a vital humanitarian aid package that was due to be delivered at 13:00 CET.

The attack rendered the United Nations Office for Coordination of Humanitarian Affairs (OCHA) and the World Food Program (WFP) in Damascus and Amman respectively offline, incapable to engage in coordination efforts.

Aleppo is in critical need of the aid package, the attack delayed efforts of humanitarian actors including the International Committee of the Red Cross (ICRC) and Doctors without Borders (MSF) in Damascus to deliver the required aid to Aleppo in due time. Simultaneously, further intelligence outline that other attacks are prominent, endangering civil society actors and their lives.

Task:

The policy teams are required to derive a response plan, in order to facilitate and ensure the delivery of the Humanitarian aid package to Aleppo from neighboring countries and cities. The groups should focus on national, regional and international cooperation, multistakeholder cooperation, capacity building to maintain a robust path for the deliverance of humanitarian aid and strengthen UN logistical servers to avoid further deterioration and targeting.

All groups are expected to highlight their cyber-policies in response to this attack and work collectively, to prevent similar aggression.

Draft Resolution on Cyberattack on UN facilities

Preamble;

Recognizing that terrorism in all forms and manifestations constitutes one of the most serious threats to international peace and security and that any acts of terrorism are criminal and unjustifiable regardless of their motivations, whenever and by whomsoever committed,

Reaffirming its commitment to sovereignty, territorial integrity and political independence of all States in accordance with the Charter of the United Nations,

Reiterating its call on the parties to allow humanitarian agencies rapid, safe and unhindered access throughout Syria, as provided for in its relevant resolutions,

Recognizing the utter most importance of maintaining global peace and world order, as aligned with the purpose and charter of the United Nations, and

In view of the claimed attack by ISIS and its ability to commit cyberattacks

We the Nation States on this Special Session of the General Assembly,

1. Urge the immediate integration to deliver Humanitarian assistance through a multi-stakeholder approach involving the Syrian Arab Republic (SAR), the European Union (EU) and the United Nations (UN), according to humanitarian international standards;

2. *Recommend* the immediate establishment of a committee of investigation composed of representatives from the SAR, EU and UN into the cyber incident, supporting the long run establishment of a policy minimizing the chances of similar events in due time;

3. Emphasize the efforts of civil actors and other stakeholders in ensuring the end of the Syrian Conflict and combating any form of terrorism.

4. *Invite* Member States to cooperate on matters of cyber resilience and capacity building;

5. *Stress* the necessity of maintaining humanitarian aid and other support tools to the Syrian people.

6. *Recommends* the Syrian Arab Republic to facilitate the establishment and arrangement of safe corridors with concerned parties, as an exceptional measure not in contradiction with its authority on its space borders.

7. *Invite* the UN to submit regular reports on progress