# Houston Area Model United Nations

## Standard Committee

# DISEC

Chair | Chandler Scott

Standard Committee Background Guide

Houston Area Model United Nations 47

January 27-28, 2022

# Copyright Notice

Cybersecurity and Cyberdefense

**DISEC Background**
The United Nations General Assembly First Committee (the Disarmament and International Security Committee [DISEC]) is a key element of the General Assembly, or GA. All countries are represented within the DISEC, as it is part of the General Assembly.

**Topic #1 Background: Cybersecurity and Cyberdefense**
According to the Cyber Security & Infrastructure Security Agency (CISA), "Cyber security is the art of protecting networks, devices and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity and availability of information."

There is growing concern over the misuse of information and communications technologies (ICT) by terrorists, in particular the Internet and new digital technologies, to commit, incite, recruit for, fund or plan terrorist acts. Member States have stressed the importance of multi-stakeholder cooperation in tackling this threat, including among Member States, international, regional and sub regional organizations, the private sector and civil society.

**Past UN Action**
In resolution 2341 (2017), the Security Council calls upon Member States “to establish or strengthen national, regional and international partnerships with stakeholders, both public and private, as appropriate, to share information and experience in order to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks on critical infrastructure facilities, including through joint training, and use or establishment of relevant communication or emergency warning networks.”

More recently, the 3rd iteration of the UN’s Open-ended Working Group (OEWG) on Cybersecurity voted and unanimously agreed on guidelines and regulations for cooperation on issues of cybersecurity and prevention of cyberattacks globally. This signals a willingness from member-states on ensuring that there is a framework to deal with the current global worry about cyber threats.

The UN Office of Counter-Terrorism (UNOCT), as part of the work of the General Assembly and consultancy of the Disarmament and International Security Committee, has several initiatives in the field of new technologies, including a project on the use of social media to gather open source information and digital evidence to counter terrorism and violent extremism while respecting human rights. It has provided expertise in

international fora on the use of unmanned aerial systems (UAS) and will develop further programming in this area.

In particular, the Cybersecurity and New Technologies programme aims to enhance capacities of Member States and private organizations in preventing cyber-attacks carried out by terrorist actors against critical infrastructure. The project programme also seeks to mitigate the impact and recover and restore the targeted systems should such cyber-attacks occur.

**Current Situation**

Estimated global losses from cybercrime are projected to hit just under a record $1 trillion for 2020 as the coronavirus pandemic provided new opportunities for hackers to target consumers and businesses.

The projection of $945 billion in losses, from a new report out today from the Center for Strategic and International Studies and computer security company McAfee, is almost double the monetary loss from cybercrime than the $500 billion in 2018.

The report underscores the growing dangers that ransomware attacks by foreign criminal enterprises posed to industry. Lawmakers have been deeply concerned about the impact of such attacks, including on the financial and health-care sectors, in the pandemic.

Beyond economic losses, information loss and theft are also of immense concern. Global powers with immense cyber-capabilities have the power to manipulate elections, as has been seen in recent, smaller powers' elections in the Global South, as well as violate the sovereignty of member-states without the power to protect themselves.

Because of the immense threat which cybersecurity poses to the economy, to democracy, and to tomorrow's future, which heavily relies upon technology, it is imperative that the United Nations Disarmament and International Security Committee focuses upon this crucial topic.

**Needed Action & Resources**

In terms of action, more research is needed in the state attacks perpetrated by state actors and hacking groups alike. The research required is two-fold: both research into tracking & detecting attacks to ensure that responsible parties are penalized to the fullest extent of international regulation and law.

Second, research into preventing the attacks by way of bolstering state security requirements and implementing such security technology into states' government databases, e-election technology, and other important dependent electronic systems.

**Responsibility**
***From the UN:***

***"Few technologies have been as powerful as information and communications technologies in reshaping economies, societies and international relations. Cyberspace touches every aspect of our lives. The benefits are enormous, but they do not come without risk. The global ICT environment is facing a dramatic increase in the malicious use of ICTs by State and non-State actors. The misuse of ICTs poses a risk for all States and may harm international peace and security."***

It is the responsibility of the Disarmament and International Security Committee (DISEC) and the United Nations to ensure that there is a framework to protect democracies against the rising tides of data breaches, electronic system manipulation, and other data crimes.

DISEC must work to bring together the tech industry, new discoveries and developments in cybersecurity, and state actors to form a more robust set of security protocols to ensure that states have the ability to protect themselves.

DISEC must also set stiff penalties for states and state-sponsored groups which involve themselves in the manipulation of data for their own gain.

**Resources**
https://www.washingtonpost.com/politics/2020/12/07/cybersecurity-202-global-losses-cybercrime-skyrocketed-nearly-1-trillion-2020/
https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what
https://undocs.org/A/RES/72/284
https://undocs.org/S/RES/2341(2017)
http://undocs.org/S/RES/2370(2017)
https://undocs.org/S/2015/939


HAMUN