Houston Area Model United Nations
Standard Committee

DISEC

Chairs | Michael Bolanos and Valeria Diaz
Topic B: Cybersecurity and the Role of Space-based Surveillance Systems
Houston Area Model United Nations 50
February 6 & 7, 2025

Atilgan Ozdil/Anadolu Ag

Note to Delegates

Delegates,

Welcome to the 50th annual Houston Area Model United Nations. My name is Michael Bolanos, and I am excited to be your chair for the Disarmament and International Security Committee (DISEC). I look forward to meeting you and having meaningful, respectful conversations with all of you!

I am currently a junior at Rice University, double majoring in Integrative Biosciences and Visual Arts on the pre-med track. At Rice, I am secretary of Crochet Club, a Peer Academic Advisor, and the social chair for Rice Swim Club. I am also part of the executive board for HAMUN this year. I have attended HAMUN for 4 years, one of them in this very committee—I really enjoyed the topics discussed and the solutions we came up with when I was in DISEC. I have also staffed for HAMUN for 2 years as a vice chair and crisis chair, and I enjoyed facilitating challenging debates. I am eager to see what this committee has to offer when it comes to creating innovative solutions to ever evolving problems.

The objective of this year's DISEC committee is to address issues relating to global peace and security. Our topics this year will look somewhat different than previous years: 1) Strengthening International Measures to Prevent and Respond to Disease Warfare and Bioterrorism, and 2) Cybersecurity and the Role of Space-based Surveillance Systems. Throughout these topics, I hope to address the issues caused by the growing field of technology, especially relating to its looming threat to national security.

I am excited to see what creative insights and solutions you guys will come up with! I know that you all will create brilliant ideas and compromises. Throughout this process, I hope you are able to strengthen your skills in eloquence and gain insight on the destruction that innovation can bring. Remember to always have fun, and again, I can't wait to meet y'all!

Michael Bolanos
Chair of DISEC
bb72@rice.edu

Note to Delegates

Delegates,

Howdy! My name is Valeria Diaz, and I am a freshman aerospace engineering major at Texas A&M. Outside of academics, I enjoy taking part in club sports like beach volleyball and tennis. I also enjoy creative arts like pottery and ceramics! I am very excited to be your co-chair for DISEC at HAMUN 50.

Junior year, I joined Model UN because I was unsure of what career to pursue. While I excelled in math and science related courses, I knew I needed an outlet where I could learn and discuss current world issues and events at my own leisure. Model UN definitely proved fruitful as it helped me come out of my shell and learn to have discussion and debate in a collaborative manner. Ultimately, Model UN helped me realize that I want to pursue a career that encourages innovation and requires the efforts of the collective rather than the individual.

I was inclined to chair in DISEC because I am intrigued on how emerging technologies can affect international peace and cooperation. As an aerospace engineering major, I am especially excited to discuss issues relating to Outer Space, but also keen on examining biowarfare this year in committee!

A tip that helped me: you can never be too prepared! I believe anxieties lessen when I am more confident in the material that I have prepared and the information I have learned about a topic. Don't think you need to memorize *everything* to do well. Remember, the most important thing you should do in a committee is have fun! If there is anything you need or require clarification on, please feel free to contact me! I look forward to meeting you all this coming February.

Best of luck!

Valeria Diaz
Co-Chair of DISEC
valeriadiaz@tamu.edu

What is DISEC?

The first committee of the Model United Nations, The Disarmament and International Security plays a pivotal role in Global Peace, military concerns, and security concerns. Since its inception in 1946, after the end of the second world war, the role of this committee is to foster cooperation between nations to ensure peace and security. As one of the largest committees at the Model United Nations Conference, this committee allows for a rich variety of perspectives and echoes the diverse global community it represents. From the first conference in 1946, The Elimination of Nuclear Weapons and The Control of Atomic Energy, to Cyber Attacks and Cyber Warfare in 2024, the topics of this committee have evolved with the growth of the technological field. It was, and still is, one of the most influential committees in the United Nations.

Background Information

The Open-Ended Working Group, established in 2018 by the UN General Assembly, was created to develop norms for states' behavior in cyberspace, and implement needed regulations regarding cyberspace as technology rapidly advances. In 2021, the group concluded negotiations on 11 voluntary and non-binding cyber norms to promote international peace and enhance security in the cyber domain.

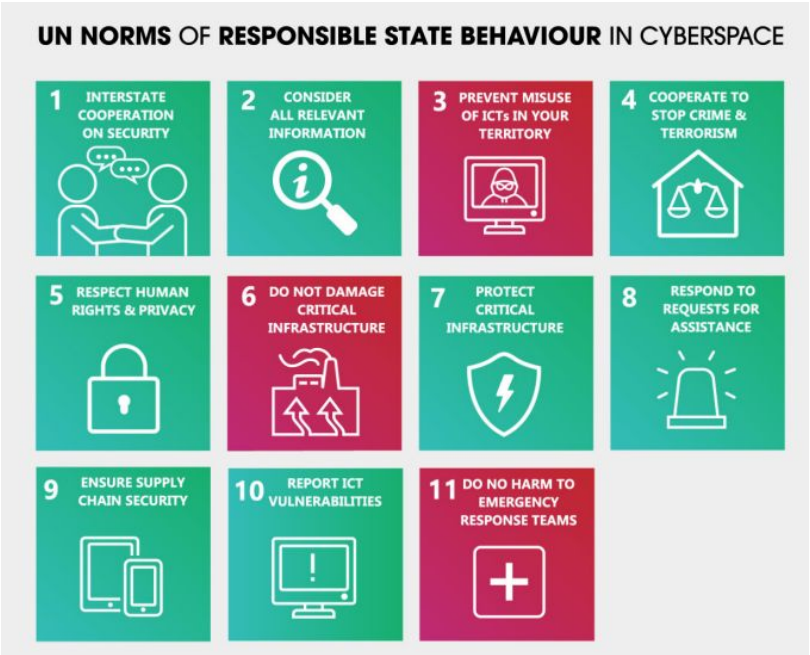

Figure 1: *11 UN Norms as a result of the UEWG*

Currently, this framework is non-binding and largely applicable to states only. In a time with rapidly advancing technology, a framework that merely suggests behavioral action to be taken has caused the international community to be doubtful that legal foundation will ever come to fruition. Additionally, with cyber attacks becoming more frequent and increasing in scale (i.e. state vs. state), the issue arises: do cyber attacks leave enough of a devastating impact to require further UN attention, and in a domain as vast as cyberspace, how can legal action be implemented? In the Chinese Cyber Espionage Campaigns of 2021, various states including the US, UK, and even NATO cited China for violating the 11 UN Norms of Responsible State Behavior in Cyberspace. Despite the public call out, neither an international statement nor corrective action was taken by UN bodies to condemn Chinese authorities. As the UN's leniency with regards to cyber attacks across the cyber domain becomes abundantly clear, tension has increased among battling governing bodies.

Unlike cybersecurity, the UN's action on space exploration, utilization of space resources, and space-based technology has been extensively covered and debated. Various GGE's, Group of Governmental Experts, have been fundamental in resolving arising space framework issues. In 2010, a GGE along with the General Assembly came to a consensus on a set of voluntary space transparency and confidence-building measures (TCBMs) to promote peaceful and the proactive use of outer space. Significant objectives includes:

1. Information exchange on space policies and activities
2. Contact and visits to space facilities
3. International cooperation and risk reduction notifications

As of recent, the UN Office for Outer Space Affairs, established in 1958, in collaboration with the General Assembly adopted the "Space2030" agenda. This agenda utilizes space and its resources to further advance the UN's 17 Sustainable Development Goals (SDGs).

While the use of outer space continues to be debated, ambiguity remains in the sector of information gathering and space-based systems. The 2017 GGE on Prevention of an Arms Race in Outer Space was tasked with considering and recommending a legally binding framework to prevent an arms race in space. Yet, it ultimately failed to reach a consensus on a final report. Thus, solid framework on the militarization of space, use of space-based systems, and weaponization of information systems has yet to be introduced and resolved.

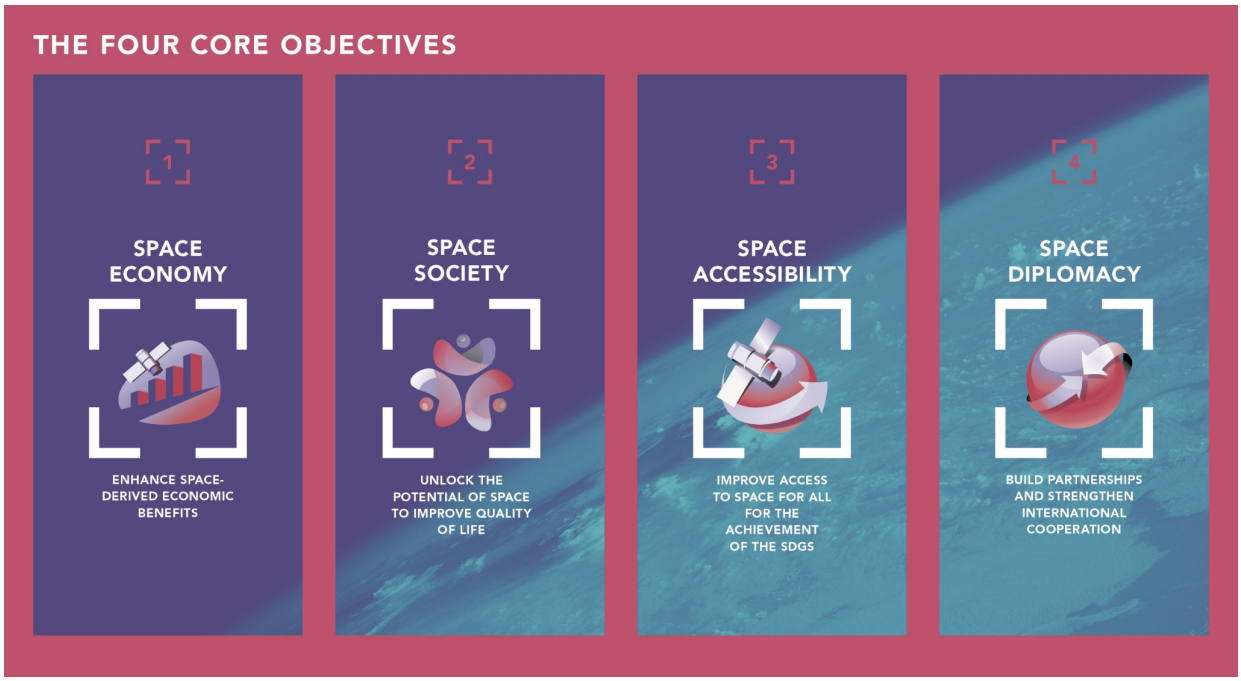

Figure 2: Space 2030 Agenda

Cybersecurity

Cybersecurity is the safeguarding of networks, devices, and data from unauthorized users. Cybersecurity systems ensure confidentiality and privacy to the user throughout the internet and private networks.

Cyberattacks are conducted via the cyberspace to intentionally disrupt, dismantle, steal, or "maliciously control a computing environment or infrastructure"; thus, a cyberattack destroys the integrity of a network putting in risk the confidentiality of data or other informations saved within the network. Additionally, there are multiple ways to conduct an attack via the cyberspace; furthermore, it makes it increasingly complicated to regulate without breaching individual freedoms.

With work and lifestyles becoming more reliant on technology, the safeguarding of an individual's privacy as well as state privacy within the cyberspace has become an issue of global concern.

One of the most covered cyber attacks of the 21st century was the 2014 Yahoo data breaches. In a spear-phishing attack, a Yahoo employee accidently gave a group of 4 hackers access to the Yahoo network. Using a backdoor to have continual access, the hackers began taking information from Yahoo's database. According the the U.S. department of Justice, the hackers gained information of more than 500 million Yahoo accounts. In the hacker's indictment, it was revealed that they were specifically targeting accounts related to government officials, banks, and military organizations.

Figure 2 : *U.S. Department of Justice charges four defendants, including two russian intelligence officers for breach at Yahoo.*

Space-based Surveillance

Space-based Surveillance Systems, not to be confused with the United States Space Force's collection of satellites of the same name, are a network of satellites and similar space-based channels used to monitor and collect information about activities on Earth and Outer Space. These systems are often used for environmental monitoring, but can serve other purposes, such as, militaristic intelligence, for navigation operations, and communication avenues.

With space-based assets becoming more common within well developed countries, their initial purposes as informative structures are challenged. Similarly, as resonance systems acquire advanced imaging capabilities, ethical questions play into the proper use of space-based surveillance. For example, inquiries on the right to privacy of an individual citizen or nonpublic business are debated when questioning the legitimacy of space-based surveillance systems operations. Furthermore, the threat of these networks being used to promote espionage provokes the very value of which the systems were built upon.

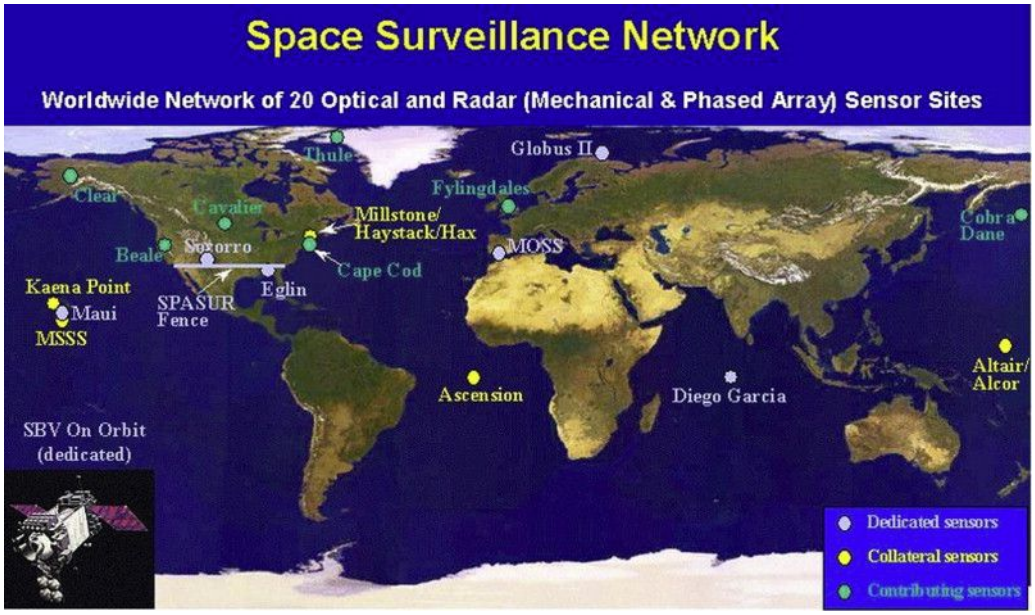

Figure 3: Network of Optical and Radar Sensor Sites Systems

Case A: 2019 Cyber attack on Georgia

On October 28, 2019, an orchestrated cyber attack on Georgian websites, including government agencies, commercial and private organizations, media, banks and financial institutions, and even personal web pages were forced offline. Defaced websites included an image replacement of former Georgian President Mikheil Saakashvili with a text reading “I’ll be back”. While former President Saakashvili was self-exiled and often accused with criminal charges, including abuse of power, from Georgia’s own, the attacks were without explicit motive for the images and text.

In the attacks, over 15,000 websites where forced offline, but various institutions suffered different degrees of attacks, with media stations and banks getting some of the worst hits. The attack, while not officially confirmed by themselves, is often attributed to Russian hackers attempting to destabilize its developing neighbors using relatively new and unprotected technologies– that is: cyberspace. Similarly, Georgia reported having faced similar misleading tactics during the initial Russo-Georgian war of 2008.

The attack reiterated the idea that cyberspace was no longer a precious commodity, but a necessary feature in daily life. The incident proved that stronger security measures were fundamental to the proper functioning of websites and databases as well as provided insight into how a cyber warfare would affect civilians’ livelihood.

Additionally, the idea of “hybrid warfare” was further explored. Using tools like attacking websites, misinformation campaigning, and the subversion and interference of financial institutions, hackers gain power over states and sabotage development through an unexpected way. While over 20 countries issued statements blaming Russia, no official international condemnation was taken.

Potential Questions

Having discussed cybersecurity and space-based surveillance systems and their intersectionality, consider the following questions. Questions are not limited to those posted below, these are just some suggestions as to what one might include in their position paper or debate. Feel free to explore ideas previously mentioned or divulge into ideas beyond, such as and not limited to, ethical and future concerns.

1. How does one balance national security concerns with privacy rights when using space-based surveillance systems?
2. What would be the ideal protocol as a response to a security threat that a space-based surveillance system would face?
3. Who should bear the economic costs of securing cyber threats in space-based surveillance systems, and how would opposing ground based alternatives factor in?
4. What are the implications of using space-based surveillance to monitor foreign countries, and how might this impact cyber retaliation?
5. How do cyber attacks on critical infrastructure affect the global economy, and how should developing countries handle the implementations of cyber security given limited resources and economic burden.
6. Consider how the UN's SDGs might contribute to the discussion of cybersecurity and space-based surveillance systems.

.

Sources

https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf

https://www.unoosa.org/res/oosadoc/data/documents/2024/stspace/stspace88_0_html/st_space-088E.pdf

https://www.cisa.gov/news-events/news/what-cybersecurity

https://csrc.nist.gov/glossary/term/cyber_attack

https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions

https://www.sciencedirect.com/topics/engineering/space-surveillance

https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/

https://www.cnn.com/2020/02/20/politics/russia-georgia-hacking/index.html

HAMUN