UN Disarmament and Security Committee

Chairs:
Edgardo Letona
Joana Nikolova

Letter from the Chairs

Dear Delegates,

We would like to welcome you to the MIT Model United Nations Conference 2020 and especially to the Disarmament and International Security Committee, or otherwise known as the First Committee. We are glad to bring to the committee the important topics of ***Regulations of Outer Space Use by Private Entities*** and ***Cybersecurity in Failed States***. We hope that together, we will be able to work productively on these topics of global importance.

We are honored to be the chairs of the DISEC Committee for the MITMUNC 2020. Edgardo is a sophomore studying Economics and Political Science and is interested in studying Development, Warfare and Political economy. Joana is a first-year intending to major in Aerospace Engineering and is interested in understanding International Relations and Policies.

We have prepared this guide to give you the basic information about the topics and the direction we have imagined the discussion might go, but this is in no way an extensive research. You should prepare yourself to represent the position of your country to the best of your ability and defend its interests throughout the whole conference. As a preparation, we will be expecting your position papers at mitmunc-disec@mit.edu.

Most of all, we hope that the conference will be a pleasant and happy experience for you. The Model UN Conference is an amazing opportunity to better understand the world we live in and understand the challenges that stand before us and how to resolve them. Hardly ever is there one single solution, most of the time there is no right solution, but everyone should be helping in the best way they can. Different countries have different interests and different opportunities and so as an International Body of Unity, the UN tries to find the best compromise. Ultimately, this is what guides the work of any committee - moving the whole world to a safer and better future.

Sincerely,
Edgardo Letona & Joana Nikolova
Chairs, DISEC

Topic 1: Regulations of Outer Space Use by Private Entities

Introduction and Background History

As our civilization continues to develop, we are developing more and more technology that allows us work in Outer Space. For decades, the only entities with the ability to send and retreat objects from outside the atmosphere were the governments of the most powerful and economically advanced countries. In recent years, however, more and more private companies are able to send their work to Outer Space - from small student projects brought with the cargo to the International Space Station, to SpaceX Rockets delivering satellites, the field of people who leave their prints outside of our planet is rapidly enlarging. However, as more and more private entities own equipment in Outer Space it becomes necessary to create a global policy on expectations of conduct.

International space policy has a long history that started with the adoption of the Outer Space Treaty of 1967 that established the international rules and expectations beyond our planet (Outer Space Treaty). This agreement is mainly focused on the responsibilities of different nation states in their work in space and designates Outer Space as a place for peaceful and collaborative exploration (Outer Space Treaty). The *Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space* puts the responsibility for actions of non-governmental entities to the States affiliated with these entities. Practice has shown that private investments in space exploration lower overall and national costs (Grady). However, this also can mean that countries may be dependent on private companies for the development of their own space programs, which might mean a legal responsibility for their actions (Grady). In this case, the responsibilities and gains are not evenly distributed (Grady).

It is important to develop a capable and responsible space policy for private entities in order to improve national security. With the increasing involvement of different parties in space, it is crucial that it is established under what rules they will be able to work together. Private projects can be of national interest if they have the potential to boost the economy or play a role in a governmental project, and this creates opportunities for international conflicts over private actions of space. At the same time, there is a question to what extent private entities can or should be able to provide autonomous access to space to governmental and non-governmental organizations.

Key Aspects:

The following are important aspects that will largely be the focus of this committee.

Military Aspect:

There is only limited control over militarization and weaponization of Outer Space. This can cause major security implications for all countries and therefore is an important aspect of global policies than needs to be recognized. Specifically, there is a need to define what are non-governmental entities allowed to bring to space. There seems to be a tradeoff between the ability to protect investments and adherence to international values of cooperation & peace. Furthermore, as private actors go to space, there needs to be a better understanding of what should be considered a militarized action. They might desire an increased security presence, but militaries are generally associated with a country, not a business or an NGO. Connected to this, there might be a need for a discussion on what are the expectations for security cooperation in space.

At the same time, space technology plays a crucial role for military actions on Earth providing surveillance, location identification, etc. It can be beneficial for some countries or private contractors to use the services of private companies that provide such services. However, this can endanger the security of other actors in Space or on Earth. Therefore, it might be crucial that there are expectations and guidelines for the activities of private entities in Space. Alternatively, there might be a need for general rules on what actions can be done on private space property from Earth actors.

Commercial Use:

The Outer Space Treaty established Outer Space as a place for all. It went as far as to establish that no country will be able to appropriate parts of Outer Space. Therefore, it remains unclear what should be the rules regarding private companies and what they can claim. On Earth, a company is given permission by the state that owns certain resources (natural resources, land, etc.), but the legal requirement for such actions in space is unclear. Even more, it can be said that allowing the privatization of space resources can violate the values of equality as access to space seems inherently unequal. At the same time, it can be argued that resources from Outer Space can provide development on Earth and improve the overall quality of life. It can be added that private enterprises may be more likely or willing to invest in such pioneering and financially insecure tasks. A global policy on the commercial use of space will require carefully balancing considerations about equality with incitements for continued work in technological development.

Law Jurisdiction and Countries Affiliated with Entities:

Currently any private actor is in the jurisdiction of the country where it is registered, which means that the state is responsible for the actions of non-governmental entities that are registered with it. This may be a factor that drives companies with goals to reach Outer Space, to refrain from hiring international participants. Furthermore, the fact that a country is liable for any damage done by its entities may be a reason for countries with smaller economic capabilities to depend on private companies.

Life and Colonization:

A particular case of questioning Jurisdiction can be seen in the colonization (Wheeling). It is well known that there is a SpaceX mission planned in the coming years that will aim to colonize Mars and extend our civilization to the Red Planet (SpaceX). However, the establishment of a society will require common rules and responsibilities, organization, control, in other words it would be governed by something. Current international law has a gray area in this topic: on one side, the Outer Space Treaty establishes that national states will be deemed responsible for the actions of their nationals (including non-governmental entities), but on the other it insists that no country appropriates any part of Outer Space. Even more, a part of a state's laws is guided by the underlying assumption that they will be implemented on territories controlled by the country. Another problem that appears when thinking about long-term missions is what would be the channels for upholding the law.

Possible Positions

The following are possible positions your delegation may align with.

USA

The Commercial Space Launch Competitiveness Act of 2015 allowed American companies to exploit outer space resources for commercial purposes. At the same time, NASA has been outsourcing many of its projects to private companies in order to reduce costs (Markovitch and Chatzky). There are propositions that NASA restructures its dealings so that they more resemble the way other US agencies create objectives and have private entities bid for the orders; but opponents of this idea claim that it may not be viable due to lack of competition in the field (Markovitch and Chatzky).

China

The Chinese government has released its guide on Outer Space activity in July 2019 and it includes specific expectations for the private industry (Jones). The country has allowed the growth of the private sector of aerospace companies that aim to explore Outer Space, but it is expected that these companies will follow the government's guidance (Jones).

European Union

The policy of the European Commission is that private activity in space can be done only if it does not interfere with science exploration (European Commission). It has an expectation for the private sector to be more "risk-prone" and "develop innovative products and services" (European Commission). Additionally, the EU states that space technology can play a crucial role in challenges such as "migration, border control and maritime surveillance", though not explicitly when talking about private companies, but it does state a readiness to invest in the private sector. The EU believes that policies strengthening transparency and cooperation will be central for ensuring safety and security around the globe (Homolkova).

Conclusion:

This committee will be trying to construct a viable global policy that concerns the actions of private entities in space. We will aim to explore to what extent, private use of Outer Space is compatible with the values of collaboration, mutual support and equality of opportunity, values that have been set by the Outer Space Treaty. It is important to consider how can the global community ensure that common goals in space are achieved in the face of the private sector that is trying to increase profits (Grady). The chairs will highly value discussions that take into account the security interest of countries without Outer Space capabilities. There is no expectation for the discussion to be limited to the proposed subtopics, they are only for your guidance.

Works Cited:

Grady, Monica. "Private Companies Are Launching a New Space Race – Here's What to Expect." *The Conversation*, The Conversation, 26 Mar. 2019, theconversation.com/private-companies-are-launching-a-new-space-race-heres-what-to-expect-80697.

European Commission. "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions." *DocsRoom - European Commission*, 23 Oct. 2016, ec.europa.eu/docsroom/documents/19442.

Homolkova, Marketa. "EU Statement – United Nations 1st Committee: Thematic Discussion on Outer Space." *EEAS*, Delegation of the European Union to the United Nations, 29 Oct. 2019, eeas.europa.eu/delegations/un-new-york/69603/eu-statement-%E2%80%93-united-nations-1st-committee-thematic-discussion-outer-space_en.

Jones, Andrew. "Chinese Commercial Launch Sector Regulations Released, New Launch Vehicle Plans Unveiled." *SpaceNews.com*, 2 July 2019, spacenews.com/chinese-commercial-launch-sector-regulations-released-new-launch-vehicle-plans-unveiled/.

Markovich, Steven J, and Andrew Chatzky. "Space Exploration and U.S. Competitiveness." *Council on Foreign Relations*, Council on Foreign Relations, 10 Sept. 2019, www.cfr.org/backgrounder/space-exploration-and-us-competitiveness.

SpaceX Staff. "Making Life Multiplanetary." *SpaceX, Space Exploration Technologies,* 20 Sept. 2016, www.spacex.com/mars.

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, 19 December 1966, *United Nations Office for Outer Space Affairs*, available from https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html

Wheeling, Kate. "Outer Space Treaties Didn't Anticipate the Privatization of Space Travel. Can They Be Enforced?" *Pacific Standard*, The Social Justice Foundation, 14 Aug. 2019,

psmag.com/social-justice/outer-space-treaties-didnt-anticipate-the-privatization-of-space-travel-can-they-be-enforced.

Suggested sources:

The WIRED Guide to Commercial Human Space Flight - https://www.wired.com/story/wired-guide-commercial-space-flight/

Space Law Treaties and Principles - https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties.html

ISS Legal Framework - http://www.esa.int/Science_Exploration/Human_and_Robotic_Exploration/International_Space_Station/International_Space_Station_legal_framework

Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States, Taking into Particular Account the Needs of Developing Countries https://www.unoosa.org/oosa/oosadoc/data/resolutions/1996/general_assembly_51st_session/ares51122.html

Charter of the UN - https://www.un.org/en/charter-united-nations/index.html

CIA World Factbook - https://www.cia.gov/library/publications/the-world-factbook/

BBC - https://www.bbc.co.uk/

Al Jazeera - https://www.aljazeera.com/

UN Documents - https://www.un.org/en/sections/general/documents/index.html

United Nation Office for Outer Space Affairs - https://www.unoosa.org/

Topic 2: Cybersecurity in Failed States

Introduction and Background History

This is the story of one of the bigger problems of modernity. The last five decades have seen incredible changes in the world's management of information, and this is because Information Technologies (IT) had a great expansion in the early 1970's in the developed countries around the world. As humankind started to understand the power of these resources, the more useful it became, for almost any discipline, to apply in some way the power of computation to the daily needs of this given discipline. These applications range from the easier management of demographic information by governments across the world, to machine learning algorithms that help private companies better target their ads for their consumers.

Unfortunately, when these technologies were starting to be developed, so too was the area of **malware** increasing. Robert Morris, now a tenured professor at MIT, developed the first computer worm in history (Ornman). In 1988, he developed a code that leaves a trace when it enters in different computer systems, demonstrating that the Internet, as a network system, was not going to be a friendly place. From there on, cybercrime has become a hot topic in almost all regions of the world.

By 2015, Brookings Institute released two studies on cybersecurity plans in US government agencies (Desouza and Fedorschak). They argue that most of the public agencies in the US lack a clear cybersecurity plan, and they recommend to address the cybersecurity threats by innovation and deeper understanding of future hazards. In addition, they claim that a failure on enhancing IT security would likely result in catastrophic outcomes as cyber vandals and militant groups target critical infrastructure. For example, in the private sector, by 2015, Target suffered a cyber-attack where hackers gained 40 million credit and debit card numbers; Home Depot as well declared that they had a payment system breach affecting 53 million individuals. While trying to seize these figures, it should become easier to understand why cybersecurity is an important strategy to reinforce the protection of the individuals. Furthermore, it is important to realize that by 2015 the United States, one of the world's leading economies and nation, was having major problems with cybersecurity in its private sector.

However, our goal here is having a discussion of the same kind of issues in **failed states**. Max Weber's definition of State is at its most basic sense, the monopoly on the legitimate use of physical force (Munro). Hence, by not enforcing it, the State becomes in charge of protecting its citizens. Since we are going to study cybersecurity, this is the basic definition we need of State. Cybersecurity should be a responsibility of the State, given the definition we gave. However, the advent of computation and all its consequences did not come evolved completely as a part of the government, it was evolved by private entities. For this reason, Jaime Collier, doctoral student in the Centre for Doctoral Training in Cyber Security at Oxford, in his work of understanding the nature of cyber security acknowledges that public-private partnerships, the role of civilian-led groups play a significant role in cyber security provision (Collier). For our discussion, it is going to be necessary to understand how these other actors shape cyber security in places where there is no State.

Furthermore, to understand cybersecurity in Failed States, we ought to look at what cybersecurity is fighting against, which is **cybercrime**. This becomes a more fundamental subject in **the Global South** (Kshetri) where most, if not all, of the failed states in the world are situated. International cyberattacks associated with the GS have complex dimensions, ranging from political conflicts that involves cyberwarfare, such as one of the first formal uses of offensive cyber weapons, the US operation "Olympic Games" which sabotaged Iranian nuclear facilities by means of cyber disruption (Nakashima), to more personal forms of threat, such as the Nigerian letters or "419" fraud which attempts to convince users to share personal information such as bank accounts or Social Security Numbers (Herring).

As the world becomes more digitized, the need for a better understanding of what a country can do, if any, to avoid cyberattacks is increasing exponentially. Especially in failed states, where there is no official bureaucracy that answers the people's need, we ought to understand how cybercrime plays a role in the daily lives of these people. At the same time, it is important to consider what are the limits of the use of cyber weapons against a region without state, because depending on these limits we would be able to infer to what extent people in failed states are protected or not against cybercrimes. Finally, why the people's protection against cybercrime is so fundamental in the study of a State, becomes as an intertwined inquiry in our discussion.

Key Aspects:

The following aspects that should be considered under the study of failed states.

Social Engineering:

Kevin Mitnick, the most famous hacker of our time, in the 1990's made popular the term of social engineering, the study on how to manage social change and regulate behavior (Hadnagy). This method of hacking is useful because it is easier to exploit the psychology of people to get information rather than searching for a weak point in the software the hacker is interested in. These methods of social engineering aim to manipulate individuals to get access of deep structures in software or hardware. By 2019, according to Computer Weekly (Scroxton), social engineering is a factor in basically all cyberattacks. Since it is easy to fall by this type of attacks, it is necessary to consider to what point people living in Failed States are protected from them and how can its citizens avoid these attacks.

Cyber Warfare:

The usage of technology in warfare has a long history, and its beginnings can be traced back to the Second World War. The "Enigma" code was used by Nazi Germany to encode its commercial, diplomatic, and military operations. This was deciphered by the efforts of the Great Britain and the United States (interestingly again, MIT's former Radiation Laboratory played a huge role in providing technology for the Allies in World War II, including computational devices, microwave and radar technologies).

Furthermore, the advances of technologies that allowed the digitalization of information made it possible for a Nation-State to attack other countries in an act of what is known as cyber war. Cyber Warfare has become significantly important in recent decades because of the attacks against Estonia in 2007, Georgia in 2008, and Iran 2010.

The issues regarding Cyber warfare in Failed States are very diverse, for instance, if a person from a failed State attacks a Country, who is this country going to declare the aggression against? Moreover, how can a Failed State defend itself from a formal cyber-attack from another country?

Espionage

Espionage is one of the most remarkable activities in human history. It has been present since ancient times and it is still in use today. Espionage can be considered as the missing dimension of historical scholarship, since it has changed the world in ways that we do not really understand. In fact, one of the first needs to develop computation was to break German coded communication as mentioned above. As the BBC's security correspondent Gordon Corera mentions that computers went from being a tool for espionage to get embedded and fused with spying activities (Corera), which means that computers shifted a paradigm in Espionage. One of the first espionage attacks done to the west was Titan Rain, that occurred from 2003 to 2005, with the purpose of systematic intrusions into hundreds of US and UK government computers and networks (Norton-Taylor). Since the increasing threat of espionage is inherited in the computational structures, it is necessary to understand how a failed State responds to Espionage, how this can affect the politics in the region.

Possible Positions

So far, we have understood the phenomena of cybersecurity. Our discussion needs to explain how the different countries in the world, interpret cybersecurity and stand in a certain position within this phenomenon. Some of the most influential blocks will be listed but it's your responsibility to research and explain your country's position.

Furthermore, the description of this position has the intent of giving the students a background and historical guide to understand the different positions and country blocks. This is not an attempt to describe the different positions and country blocks today.

European Union (EU):

The EU was one of the earliest advocates of the information society. By 2010, the EU had a well-established legal and policy framework in regards to instruments involved with IT (Tikk). By that time, different governments around the world adopted the EU policy framework regarding IT. Since it was the first International Alliance that considered IT security as a part of their policy-making. By 2010, the EU had an advantage in the international cybersecurity arena, by establishing the first guidelines regarding cybercrimes and general Internet governance.

NATO:

After the first cyber-attacks against Estonia in 2007, NATO and several military authorities in the Globe started to get involved in strategic cybersecurity planning (Tikk). In addition, NATO's approach to cybersecurity, assumes that the first steps of cybersecurity cooperation are significant information society agendas in the local politics regarding this issue. Hence, a response against a cyber-attack to a Nation might be evaluated by considering the National efforts on cybersecurity. Furthermore, NATO, as a military-political, alliance, focus their efforts on responses and coordination of cyberattacks. Finally, by 2010, the UN and NATO were the only international organizations that were part of coordination of individual and self-defense in case of cyber armed attacks.

China:

Cyberspace was and continues to be a facilitator of China's emerging power in the twenty-first century (Lindsay). In addition, China has presented a threat against the West. For instance, the response of the US and Australia to ban Huawei and ZTE devices from sensitive systems. On the other hand, China's authorities stress the importance of informatization and cybersecurity as dual key goals to modernization. Moreover, there have been times that Western intelligence services were penetrating Chinese networks. China's national cyber-security policies were first laid out in the 2003 State Information Leading Group (SILG). Both China and the United States consider each other as a threat to their economy and military power, this relation gets more polarized as people across the world has become more dependent on IT.

USA:

Along this prompt, there has been an emphasis on the US acts in regard to its policies in the cybersecurity field. It is expected that this would be taken as a guide to understand the United States position.

Conclusion:

The purpose of this Committee is to better understand the positions of different country blocks in regarding to cybersecurity in Failed States. Furthermore, we would try to understand how can different Coalitions agree on how to proceed when a Failed State is being under a cyber-attack or is the source of cyber-attacks.

As we have discovered so far, cybersecurity is not only in the hands of Governmental regulations, the private sector and its goals in different countries play an important role in topics of cybersecurity. Hence, at the moment of learning about each country's position, we have to consider what is the say of the economic elites in this country, and further consolidate these views with the views of the public sector.

As societies have become more dependent on IT, cybersecurity plays a fundamental role in the future of humankind. As a last purpose of this topic is to understand how we are affected by cybersecurity policies that are being discussed in the international arena, and how we can, as individuals, contribute to a safer and more protected environment against malware.

Works Cited:

Orman, H. "The Morris Worm: A Fifteen-Year Perspective." *IEEE Security Privacy* 1, no. 5 (September 2003): 35–43. https://doi.org/10.1109/MSECP.2003.1236233.

Desouza, Gregory Dawson and Kevin C. "How State Governments Are Addressing Cybersecurity." *Brookings* (blog), November 30, 2001. https://www.brookings.edu/blog/techtank/2015/03/05/how-state-governments-are-addressing-cybersecurity/.

Fedorschak, Kevin C. Desouza and Kena. "The Vast Majority of the Government Lacks Clear Cybersecurity Plans." *Brookings* (blog), November 30, 2001. https://www.brookings.edu/blog/techtank/2015/02/03/the-vast-majority-of-the-government-lacks-clear-cybersecurity-plans/.

Munro, André. "State Monopoly on Violence | Political Science and Sociology | Britannica." Accessed November 29, 2019. https://www.britannica.com/topic/state-monopoly-on-violence.

Collier, Jamie. "Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision." *Politics and Governance* 6, no. 2 (June 11, 2018): 13. https://doi.org/10.17645/pag.v6i2.1324.

Kshetri, Nir. *Cybercrime and Cybersecurity in the Global South*, 2013.

Nakashima, Ellen, and Joby Warrick. "Stuxnet Was Work of U.S. and Israeli Experts, Officials Say." *Washington Post*, June 2, 2012, sec. National Security. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

Herring, Susan C., Dieter Stein, Tuija Virtanen, and Wolfram Bublitz, eds. *Pragmatics of Computer-Mediated Communication*. Handbooks of Pragmatics, ed. Wolfram Bublitz ...; Vol. 9. Berlin: de Gruyter Mouton, 2013. P.. 420

Hadnagy, Christopher. *Social Engineering: The Art of Human Hacking*. Indianapolis, IN: Wiley, 2011.

Scroxton, Alex. ComputerWeekly.com. "Social Engineering a Factor in Virtually All Cyber Attacks, Report Claims." Published 09/09/2019. https://www.computerweekly.com/news/252470384/Social-engineering-a-factor-in-virtually-all-cyber-attacks-report-claims.

Corera, Gordon, and Gildart Jackson. *Cyberspies: The Secret History of Surveillance, Hacking, and Digital Espionage*, 2016. https://www.overdrive.com/search?q=65BA7C2E-751C-4B6D-919A-012450DE8FE5.

Norton-Taylor, Richard. "Titan Rain - How Chinese Hackers Targeted Whitehall." *The Guardian*, September 5, 2007, sec. Technology. https://www.theguardian.com/technology/2007/sep/04/news.internet.

Tikk, Eneken. "Global Cybersecurity–Thinking About the Niche for NATO." *SAIS Review of International Affairs* 30, no. 2 (2010): 105–19. https://doi.org/10.1353/sais.2010.0012.

Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron, eds. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. New York: Oxford University Press, 2015.

Suggested sources:

UN GEE (Group of Governmental Experts) and OEWG (Open-Ended Working Group) in the Field of Information and Telecommunications in the Context of International Security: https://dig.watch/processes/un-gge

Organization of Security and Co-operation in Europe (OSCE): https://www.osce.org

North Atlantic Treaty Organization (NATO): https://www.nato.int

Resolutions in G7 forums

Organization for Economic Co-operation and Development (OECD): https://www.oecd.org/about/

Budapest Convention on Cybercrime: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

The Shanghai Cooperation Organization (SCO): http://eng.sectsco.org

UN World Summit on the Information Society (WSIS): https://www.itu.int/net/wsis/