



Stanford Model United Nations Conference 2014

Disarmament and International Security UN General Assembly First Committee



Chair: TBA

CoChair: Gabriel Rosen-Duran, grd@stanford.edu

Welcome to the Disarmament and International Security Committee of the United Nations!

We're very excited to have you all at the Stanford Model United Nations Conference 2014! This is going to be an excellent committee with a lot of learning and a lot of fun!

A quick note on the chairing situation: unfortunately, our original chair is no longer able to chair this committee. We will have a replacement chair in the next week. When we do get a replacement chair, we will include an updated chair letter with your chair's email address so that you can turn in background guides and ask any questions you may have. In the mean time, feel free to ask your cochair, Gabriel, or either of us any questions!

Sincerely,

Brandon Baum, Secretary General
brandonbaum@stanford.edu

Tim Wu, Undersecretary General for General Assemblies
thsuanw@stanford.edu

Topic 1: International Security, the Internet, Terrorism, and Non-State Actors

Introduction:

As the world grows increasingly connected, businesses move more of their data and activities online, cities adapt smart infrastructure, and government agencies continue to turn to the internet to carry out ever more work, the potential damage and chaos caused by a cyber attack or cyber terrorism continues to grow. While much media attention focuses on cyber warfare between states, the Internet's ubiquity and reach means that non-state actors can play an equally catastrophic role in upending international security through cyber attacks.

The threat cyber crime by non-state actors plays goes beyond explicit cyber terrorism. The Internet has also increased risks to international security by easing access of terrorist and other destabilizing and violent organizations to capital and black markets around the world and giving them a powerful tool for communication, research, and recruitment.

The first topic of debate for this body is the creation of an international policy to deal with the many threats to cyber security posed by non-state actors.

Cyber Terrorism:

There is considerable debate today about what constitutes cyber terrorism. Terrorism is defined primarily as “violent acts or acts dangerous to human life” that “appear to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping.”¹ If we stick to this specific definition then cyber terrorism would refer only to crime, which targets lives using the Internet, such as hacking into programs used by flight controllers or disrupting “smart infrastructure.” Many prefer a more broad definition: the Technolytics Institute defines it as “the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives.”² By this definition any malicious disruption of computer systems constitutes cyber terrorism. A baseline for debate should be defining cyber terrorism, and any resolutions you pass as a committee will do so, explicitly or implicitly.

Key Areas of Concern:

There are a number of uses of the Internet with regard to terrorism. These each relate to terrorism in a different way and to a different extent. It is up for the committee to decide which issues are appropriate to discuss in a resolution addressing this topic.

¹ FBI, *Definitions of Terrorism in the US Code*, <http://www.fbi.gov/about-us/investigate/terrorism/terrorism-definition>

² DCSINT Handbook 1.02, *Cyber Operations and Cyber Terrorism* <http://oai.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA439217> (Really great source for further reading)

Planning, Research and Recruitment:

The Internet has given a number of terrorist organizations a secure way to communicate. This is an invaluable tool for both planning of events and recruiting new members. Terrorists make use of chat rooms, voice over the Internet protocols, and other means of online communication to circumvent traditional surveillance techniques. In addition, the Internet connects terrorists to thousands of pages of information, allowing terrorist organizations around the world “to gather information on any subjects that they need to research... using very simple resources.” Such information includes everything from DIY instruction manuals for producing bombs to information on the “critical infrastructure of the United States.”³

Dr. Xiao Lung Chin who recently conducted a study of terrorist recruitment on the Internet concluded, “The terrorists are at least as good as the US governments in terms of utilizing the Internet technologies to actually do propaganda and attract people to their groups.”⁴ One of the biggest challenges in passing any policy to regulate cyber communication is the movement of organizations to the “Dark Web.” One concern is that as “regulation of Surface Web sites pushes terrorists deeper in the Web,... it limits how many people can see their sites, but also makes it harder for law enforcement to track the sites.”⁵

Another issue with regulating Internet communications is the challenge it poses to human rights. As the revelations by whistleblower Edward Snowden brought up, governments attempting to regulate terrorism may resort to unpalatable levels of surveillance such as the NSA’s mass data collection programs. This is an issue particularly divisive among governments, especially as many governments have tried to distance themselves from the public outcry against the United States’ intrusions while quietly maintaining national security interests. Furthermore, many attempts to regulate information freely available on the web walk a fine line between security and censorship, especially in states whose governments tend towards authoritarianism. As chair, I expect any resolution to address these issues. While real world diplomats may stray from this issue, it is your duty to find solutions.

Money Laundering and Financing Terrorism:

Another challenge relating to international security and the Internet is the access to capital and black markets it provides. The rise of crypto currencies such as Bitcoin, which have excited those wary of government by providing an alternative to a government regulated money supply, has allowed terrorists a means to anonymously transfer money as well as access to markets.

³ DCSINT Handbook 1.02, *Cyber Operations and Cyber Terrorism* (see above for URL)

⁴ NPR, *Terrorists Manipulate ‘Dark Web to Spread Jihad’*
<http://www.npr.org/templates/story/story.php?storyId=6664425>

⁵ *Dark Side of the Web, Jihad and Terrorism on the Dark Web*,
<http://davidenewmedia.wordpress.com/subcultures/jihad-and-terrorism-on-the-dark-web/>

The recent closure of the Silk Road, an anonymous online marketplace which carried out transactions in Bitcoin and was popular for buying drugs, guns, and other illegal goods highlighted this problem. According to the FBI, the site was used primarily to facilitate illicit activities and was used by terrorist organizations to sell drugs to consumers around the world and finance their operations. Such regulation is difficult because as one site is shut down, often another springs up. Furthermore, the decentralized nature of Bitcoin means it can be used to transfer money without any single website facilitating the transaction.



However, when such regulation is effective, it is subject to a flurry of controversy. *The Atlantic* begged the question, “Did shutting down the Silk Road make the world a more dangerous place?”⁶ Many saw this regulation as another example of governmental overreach and an affront to “free markets and human freedom.”⁷ As a delegate you must consider your country’s position carefully and strike a balance between the preservation of “human rights” and international security.

Cyber Attacks:

The final topic we must address in the field of cyber terrorism is the cyber attack itself. These attacks have one of four primary objectives: (1) loss of integrity, ie. the manipulation of data, (2) loss of functionality, (3) loss of confidentiality, or (4) physical destruction, the use of the internet to create physical harm. FBI Director James B. Comey testified to Congress in 2013 that “Internet-related attacks, espionage, and theft” will become “the most consuming security issue for the US” in the next 10 years.⁸ As *Popular Science* points out, “Cyber is very different from other threats, and needs to be treated accordingly.” Most cyber crime will “look more like crime or spycraft.”⁹ Crime will target information seizure and affect businesses on a broad level. The biggest physical dangers of cyber crime relate to disruption of critical infrastructure, which “make extensive use of computer hardware, software and computer systems.” Potential attacks could include “disruption of the rail system,... a successful attack against a power substation,... or a successful attack against telecommunications systems” that impacts

⁶ *The Atlantic*, *Did Shutting Down...* http://www.theatlantic.com/technology/archive/2013/10/did-shutting-down-silk-road-make-the-world-a-more-dangerous-place/280270/?single_page=true

⁷ *The Dollar Vigilante*, *The Shutdown that Really Matters: The End of the Silk Road*, <http://dollarvigilante.com/blog/2013/10/3/the-shutdown-that-really-matters-the-end-of-the-silk-road.html>

⁸ *Washington Post*, *FBI Director Warns of Cyberattacks...* http://www.washingtonpost.com/world/national-security/fbi-director-warns-of-cyberattacks-other-security-chiefs-say-terrorism-threat-has-altered/2013/11/14/24f1b27a-4d53-11e3-9890-a1e0997fb0c0_story.html

⁹ *Popular Science*, *Cyber Attacks are America’s Top Security Threat. That’s Better News Than it Sounds*. <http://www.popsci.com/technology/article/2013-03/cyber-attacks-were-named-top-security-threat-%E2%80%99s-better-news-it-sounds>

movement of equipment, people, or information and could be used effectively in conjunction with a more traditional threat.

Conclusion and Your Job

Clearly the Internet brings up a myriad of challenges and concerns for international security. I could have easily written a dissertation worth of material for this background guide. Instead, I have chosen to highlight a few key areas that I hope to see each of you address.

Your next step in any research is to explore what kind of existing legislation and agreements there are on both domestic and international levels. Then you should explore your country's position on the topic more thoroughly. For many of your countries, there may not be a lot of information readily available. However, if you research which bloc your country typically falls in for matters of international security and human rights, you should get a strong idea of your position.

Additional areas/questions for research include: *specific actors involved, the distinction between "hactivism" and terrorism, the role of an international body in providing a forum for such issues, and the fundamental human rights concerns with any kind of regulation.*

Topic 2: Preventing Arms Race in Outer Space

Introduction: the Race to Space

The U.S. space program was initiated in 1961 when President John F. Kennedy challenged the nation to claim a leadership role in space and land a man on the Moon before the end of the decade. The Soviet Union, America's rival in the Cold War, had surged ahead of the United States with spectacular achievements in space that struck fear into the hearts of many American citizens. Soviet leaders hailed these feats as a triumph of Communism. When a leading American physicist was asked what would be found on the Moon, he replied, "Russians."

Space exploration began at the climax of the greatest arms race in the history, after which people had been living under the shadow for 50 years. On October 4, 1957, the Soviet Union launched the satellite Sputnik 1, the first unmanned space mission, making outer space a new arena for big powers to demonstrate their military. After the Soviet Union launched two successive satellites, the Americans launched their first satellite, Explorer 1, on January 31, 1958. To sustain the leading position, Russia carried out a more ambitious mission and successfully brought Yuri Gagarin into space on April 12, 1961, and once again Americans fell behind. Against the backdrop of the strained competition between these two leading powers, it was impossible for scientists and politicians to ignore the Moon. On July 20, 1969, Neil Armstrong made the first moon walk and famously remarked "That's one small step for a man; one giant leap for mankind." The historic achievement secured the American's leading position in this round of "space race" and Russia lost its upper hand.

From what has been discussed above, we can conclude that gaining the lead in the arms race and demonstrating scientific achievements were the original intentions of devoting efforts into one after another costly and risky missions. It explains the concern for great powers making space another battlefield. Any sign of an arms race in outer space could possibly disturb the strategic balance and regional stability as well as frustrating efforts on disarmament and arms control, especially referring to countries related to nuclear weapons and ballistic missiles¹⁰.

History of the Problem:

The most effective international tool to prevent an arms race and act of aggression is Space Law. Space law, including treaties, conventions, agreements, and regulations, is the body of law, providing guidelines on space activities and promoting rational and responsible use of outer space.

In 1957, the Resolution 1148¹¹ passed by General Assembly marked the first collective efforts on the topic. In the Resolution, the operative clause 1 sub-clause (f) "the joint study of an inspection system designed to ensure that the sending of objects through

¹⁰ China's National Defense in 2004, http://english.gov.cn/official/2005-07/28/content_18078.htm Sanger, David and Bumiller, Elisabeth. "U.S. to Pull Out of ABM Treaty, Clearing Path for Antimissile Tests." New York Times. <http://www.nytimes.com/2001/12/12/international/europe/12MISS.html>

¹¹ UN GA Resolution A/RES/1148, [http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/1148\(XII\)&referer=http://www.un.org/depts/dhl/resguide/r12.htm&Lang=E](http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/1148(XII)&referer=http://www.un.org/depts/dhl/resguide/r12.htm&Lang=E)

outer space shall be exclusively for peaceful and scientific purposes” states the basic principal of space exploration.

In 1967, the Outer Space Treaty¹² was adopted by the General Assembly. As the primary legal-based agreement on outer space activities, the Treaty addresses a variety of diverse matters, which were settled and expanded later by other treaties. In the Treaty, the use of nuclear weapons and any other weapons of mass destruction, along with the military activities, such as the establishment of military bases, the testing of any type of weapon and the conduct of military maneuvers, on the Moon or any other celestial bodies are all outlawed. States are prohibited to claim the sovereignty of outer space, including the Moon and other celestial bodies, and states are also responsible for not only space activities conducted by government agencies but also by private sector.

In 1972, the Liability Convention¹³ was adopted. The Convention clarifies the liability of damage caused by manmade space debris and spacecraft, and specifies that the “launching state” bears the obligation to compensate for the damage caused by its space objects or component parts. The claim for compensation can only be put forward through diplomatic channels, the courts, or administrative tribunals of a launching State.

In 1976, the Registration Convention¹⁴ entered into force. The Convention requests States to provide UN with information of their launches, and is currently the most essential Transparency and Confidence Building Measure (TCBM).

In 1979, the Moon agreement¹⁵ expanded Article II and Article IV of the Outer Space Treaty, which refrains States from claiming sovereignty of the Moon and other celestial bodies, and forbids all forms of military activities on or around the Moon and other celestial bodies respectively.

Possible Solution

The current collective international measure to prevent further weaponization in outer space is the Transparency and Confidence Building Measures (TCBMs)¹⁶. The TCBMs were promoted during the Cold War to diminish the mistrust between the two blocs. They include the Information Exchange Measures, the Observation and Verification Measures, and the Military Constraint Measures. The Information Exchange Measures consist of the establishment of a hotline between top officials, aiming at promoting better communication. The Observation and Verification Measures focus on the sharing of the military information, in order to ensure that the intention of military activities is in conformity with UN Charter. The Military Constraint Measures are comprised of the establishment of demilitarize and weapon-free zones to prevent surprise military attacks. Nevertheless, as having been pointed out, the loophole in the

¹² Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies,

<http://www.oosa.unvienna.org/oosa/SpaceLaw/outerspt.html>

¹³ Convention on International Liability for Damage Caused by Space Objects,

<http://www.oosa.unvienna.org/oosa/SpaceLaw/liability.html>

¹⁴ Registration of Objects Launched into Outer Space,

<http://www.oosa.unvienna.org/oosa/SORegister/regist.html>

¹⁵ Agreement Governing the Activities of States on the Moon and Other Celestial Bodies,

<http://www.oosa.unvienna.org/oosa/SpaceLaw/moon.html>

¹⁶ Confidence Building, <http://www.un.org/disarmament/convarms/infoCBM/>

Registration Convention thwarts the efforts of TCBMs. In 2011, the UNGA adopted the Resolution 65/68 to establish a group of governmental experts (GGE) for searching alternatives for TCBMs. The GGE commenced its mandate in 2012, and concluded its work on 12 July 2013¹⁷.

However, the TCBMs cannot replace the role of the binding treaties. In 2002 Russia and China proposed a Working Paper on “Possible Elements for a Future International Legal Agreement on the Prevention of the Deployment of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects”¹⁸ on the Conference of Disarmament, where disarmament treaties are adopted, and brought up a draft treaty on “Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects”¹⁹ in 2008. Both of the Russian-Chinese joint proposals were dismissed by the Bush administration since they prohibit all kind of weapons from being placed in orbit, which is against the US missile defense strategy at the time.

Key Areas of Concern

However, the current legal framework requires further clarification on critical issues to keep outer space intact and to eliminate the unhealthy arms race.

The Outer Space Treaty does not provide any definition for outer space. There does not exist a clear line to separate atmosphere from outer space. Without a clear definition of outer space, it would be difficult to determine what weapons should be categorized as “Space Weapons”, whose development and deployment should be regulated for the prevention of an arms race. As such, the Outer Space Treaty, even though it recognizes the exploration and use of outer space for peaceful purposes as the common interest of all mankind, does not forbid the installation of conventional weapons or any object carrying conventional weapons in the orbit around the Earth. The interpretation of “peaceful purposes” is divided on whether all military usage, including applications of navigation and reconnaissance, should count.

Secondly, the specific timeline that states should abide by and provide the information is not mentioned in the Registration Convention. What the Convention requests is for states provide the information as soon as practicable. States might take advantage of this loophole to evade the obligation adopted in the Convention.

Lastly, the Moon Agreement is not widely ratified, and there is no sign of establishing the international regime to govern the resources of the Moon as common heritage of mankind.

Your job is to overcome these difficulties, and find a way to resolve this issue diplomatically and peacefully.

¹⁷ UN Group of Governmental Experts On Transparency and Confidence Building Measures in Outer Space Activities Concludes Its Works, <http://www.un.org/News/Press/docs/2013/dc3441.doc.htm>

¹⁸ CD/1679,

<http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G02/624/84/PDF/G0262484.pdf?OpenElement>

¹⁹ CD/1839, <http://daccess-ods.un.org/TMP/3651433.58707428.html>