WHSMUN 2019
United Nations General Assembly
First Committee (Disarmament and International Security)

Wisconsin Model United Nations
UW Milwaukee International Affairs
March 21-22, 2019
Introduction

1. Topic 1.1: Orbital Nuclear Weapons and the Militarization of Space
2. Topic 1.2: The Future of Nanotechnology
3. Topic 1.3: 21st Century Cybersecurity Challenges
4. Topic 1.4: Asymmetric Warfare in the 21st Century

Greetings Delegates!
We’re excited for the return of the General Assembly’s First Committee (Disarmament and International Security) to WHSMUN 2019. The first committee of the United Nations General Assembly addresses the maintenance of international security and the governing of disarmament. Combatting threats to the international community and challenges of the international security regime require international cooperation as well as proficient knowledge of individual nations’ capabilities and limitations. A general knowledge of the capabilities and limitations of global states will aid delegates in their research of the four subcommittee topics: Orbital Nuclear Weapons and the Militarization of Space, The Future of Nanotechnology, Cyberterrorism in the Age of the Internet, and Asymmetric Warfare in the 21st Century.

The WHSMUN 2019 staff has been working diligently for the past year to write and gather materials to best prepare delegates for our conference. This background guide should serve as an introduction to individual research, and although it is not required, the best background guides consult external sources. In order to be considered for an outstanding research award, position papers must be submitted to the WHSMUN website by March 1, 2019 at 11:59 PM. On the WHSMUN website, delegates can also find tips and the guidelines for writing efficient position papers.

Questions unable to be answered by this background guide or the WHSMUN website can be directed to wisconsinhighschoolmun@gmail.com. We wish you luck in preparation and can’t wait to see you in March!

With diplomatic courtesy,

The WHSMUN 2019 Secretariat
Topic 1.1: Orbital Nuclear Weapons & the Militarization of Space
1st Main Committee

Since Neil Armstrong first stepped on the moon on July 20th, 1969, the question of the legality and usage of space and the technology invented therein has been a question that has plagued the International Community. Peaceful uses of space have been suggested as early as 1958 in the United Nations Committee on the Peaceful Uses of Outer Space, to draft the first resolution on international outer Space Law. Culminating in the 1967 Outer Space Treaty forbidding the use of nuclear arms in Earth’s orbit as well as any astral bodies, including the moon, the International Community has been attentive to both the technological advances in regard to the Final Frontier, but wary of the devastating possibilities that could arise from military maneuvers in the lower atmosphere.

Other treaties that run parallel to the 1967 Outer Space Treaty include the Anti-Ballistic-Missile (ABM) Treaty that was made between the US and Soviet Union, limiting the usage of both nations’ ABM systems to within the atmosphere of the planet. The United States, however, withdrew from the treaty in 2001 under the Bush administration. In addition, in the United Nations Conference on Disarmament (CD) proposed the adoption of a multilateral agreement on the Prevention of an Arms Race in Outer Space (PAROS), but it has been deadlocked since 1998 by opposition from United States to any and all capitulation.

While most nations generally agree with the ban on militarization of space, the issue arising with this topic comes in the lack of definition of what “peaceful usage of space” means in the context of international politics. Thus, while nations generally equate “non-aggressive” with “peaceful” usage of space, there is no definition of where “peaceful” ends, especially considering the potential for space to be used for communication and intelligence in the Information Age.

Other United Nations bodies tasked with adjudicating on the militarization of space include the UN Committee on the Peaceful Uses of Outer Space (COPUOS), notable for its drafting of almost all legal documents that were passed by the General Assembly on the UN’s stance on Space Law, and the UN Institute for Disarmament Research (UNIDIR), which engages in research for the purpose of international security and disarmament issues. Non-state actors in this arena include the European Space Agency (ESA), an international organization of 17 member states that coordinates the financial resources and logistics of space flight for member states, the European Centre for Space Law (ECSL), created for the awareness and understanding of Space law legal frameworks, and the European Space Policy, created by the European Union, that oversees European Space policy as a whole.

Topics for Consideration:
1. In the context of the Information Age, what should be considered and constitutes the national sovereignty of a nation?
2. Considering the possibility of using them to surveil other nations, to what extent may satellites be considered a “peaceful usage of space”?
3. Parallels have been drawn between Maritime Law, most commonly known as the Law of the Seas, and Space Law. In what way would the legalities of Space usage have to be changed from that of earth-bound laws?
4. To what extent does “peaceful usage” extend? Would things such as telecommunication satellites owned by private corporations fall under the purview of the nations in which they are hosted? If so, in what way?

5. In the event that a military operation within earth’s atmosphere becomes technologically feasible, would the rule of engagement be the same as that on the ground?

Bibliography:


Topic 1.2: The Future of Nanotechnology in Weaponry and Warfare

1st Main Committee

Warfare throughout its history has constantly shifted. Initially, it was defined as a clash of two armies with simple weapons and tactics, but gradually it has evolved. During World War I, the international community saw the invention and effective implementation of chemical weapons, and during World War II, it saw the development and deployment of the first nuclear weapons. In the 21st century sociopolitical landscape, it is bearing witness to the development of the next step in warfare: nanoweapons.

Nanoweapons are best defined as falling into one of two categories; weapons that exist on an incredibly small scale, ranging from 1 to 100 nanometers, or weapons that inflict damage on that scale. Due to their small size, the tactical advantage of researching and employing nanoweapons is immense. While nanotechnology is not inherently militaristic in nature, it is speculated that advancements in this field could allow for an increase in the effectiveness of weapons that are currently at the disposal of the international community. This includes a relative increase in the potential potency of Weapons of Mass Destruction (WMD) that are currently available, such as chemical and nuclear weapons, which would be brought on by the higher difficulty of effectively detecting them and preventing their usage. Additionally, nanoweapons themselves can be developed into WMDs as explosive microdust, microbots that attack individuals, or inhaled microtubules that suffocate their targets. This is not to say that nanotechnology itself is inherently bad, it could also be effectively used to combat biological and chemical weapons if they were to be deployed.

The problems presented by the development of nanotechnology as an offensive tool are exaggerated by the fact that they are not currently explicitly restricted in any international arms treaty. This lack of explicit discussion is illustrated by the issues presented by the alleged use of DIME (Dense Inert Metal Explosive) weapons by Israel in 2009 during their military attacks on Gaza. DIME is a weapon that was developed by the United States Air Force in order to allow for the deployment of a low range, low collateral damage explosive. It focused on the dispersal of heavy metal tungsten alloy, a highly lethal substance, in approximately a four foot area. This type of weapon is theoretically addressed by Protocol (I), which was adopted in 1980 and regulated the use of weapons that left behind no substances or damage that could be detected by visual inspection, however its proponents argued that because it could be detected by an x ray, it was permissible under international law. This speaks to the problematic state of current regulations on nanoweapons.

Another issue arises with the verbiage of conventions restricting the use of biological and chemical weapons, which are incredibly dangerous when paired with nanotechnology. The issue stems from the fact the Biological Weapons Convention does not restrict the development of biological weapons based on what they are, but on what they are intended to do. This creates an environment in which biological technologies can be freely developed, but it makes enforcement of restrictions difficult.
Topics for Consideration:

1. What is the role of the international community, and specifically this body, in ensuring the safe development of nanotechnology?
2. What role should current arms conventions play in the potential development of treaties or international agreements regarding nanotechnology, specifically in relation to weaponry and warfare?
3. Should the regulation of weaponry that was seemingly regulated by previous agreements, such as the DIME weapon, be reassessed? If so, how?
4. What actions can be taken to make sure that nanoweapons do not fall into the hands of non-state actors?
5. To what extent, if any, should states developing nanotechnology be required to divulge their advancements and the subjects of their research?

Bibliography:


Topic 1.3: 21st Century Cybersecurity Challenges

1st Main Committee

Throughout the past several decades, the internet has emerged as a new battlefield. The internet and networked computers are now ubiquitous throughout all facets of modern society. In addition to e-commerce, computers are utilized to regulate vital societal services such as the electric grid and other utilities. These databases and systems have become an extremely attractive target for state sponsored cyberwarfare. A variety of nations engage and sponsor cyberattacks, including Russia, China, North Korea, and Iran.

In addition to attacks on government networks that seek to reveal classified information, civilian institutions are also at risk. These attacks can have extreme consequences even beyond the loss of data. For example, “In August [2017], a petrochemical company with a plant in Saudi Arabia was hit by a new kind of cyberassault. The attack was not designed to simply destroy data or shut down the plant…It was meant to sabotage the firm’s operations and trigger an explosion” (Perlroth & Krauss). While the August 2017 attack failed due to a coding error, the degree of the hacker’s success is problematic, as similar industrial control systems are utilized worldwide. In October 2018, a report from Bloomberg Businessweek revealed a startling new type of cyberwarfare pioneered by China; operatives from a People’s Liberation Army unit successfully infiltrated the hardware supply chain. Chinese operatives were able to install an additional tiny microchip into hardware at the factory that allowed for a backdoor into any affected networks. The tampered hardware “eventually affected almost 30 companies, including a major bank, government contractors, and the world’s most valuable company, Apple Inc.” (Robertson & Riley). Overall, as technology advances and becomes even more integrated within modern society, it can be expected that there will be both an increase in attacks and innovation in the methods that are utilized.

The numerous bodies of the United Nations have taken various actions to address cybersecurity and cyberwarfare. However, it is important to note that “up until now, no resolutions concerning cybersecurity issues have been adopted by the UNSC” (CCDOE). Draft resolutions regarding cybersecurity that originated from DISEC, ECOSOC, and SOCHUM have all reached the General Assembly. In DISEC, Russia has annually introduced nonbinding resolutions since 1998, and since 2001 has endorsed the establishment of a Group of Governmental Experts (GGE). The GGE consists “of experts from 15 states, chosen on equitable geographical distribution, for a study to consider existing and potential threats in the sphere of information security and possible cooperation measures to address them” (CCDOE). GGE have met in 2004, 2009, 2011, and 2014, and all except the first one have been able to produce a consensus report. Another development is the launch of a Global Cybersecurity Index (GCI) by the United Nations International Telecommunications Union. “First launched in 2014, the goal of the GCI is to help foster a global culture of cybersecurity…This second iteration [2017] of the GCI measures the commitment of ITU Member States towards cybersecurity in order to drive further efforts in the adoption and integration of cybersecurity on a global scale” (International Telecommunications Union). Overall, “although the aforementioned annual resolutions and the reports by the GGE can be viewed as a sign of growing consensus, there is no common understanding on how exactly the existing international law should apply to cyberspace, and the development of new global cyber norms has been limited” (CCDOE).
Overall, the largest impediment to development in this policy area is the apparent hypocrisy of certain countries. Few countries, if any, are against the development of cybersecurity. However, inconsistent actions present a barrier to change. For example, despite the act that Russia sponsors the annual legislation in DISEC, “it is widely agreed that Russia is one of the most – if not the most – accomplished nations in the world in its ability to perform state sponsored attacks, disinformation and espionage” (O’Flaherty). The United States has been skeptical at attempts to draft an international treaty regarding cybersecurity for several reasons. American representatives have noted that a framework would most likely not prevent countries such as Russia or China from acting through third parties. In addition, concerns have been raised that a treaty could potentially “limit the freedom of information under the guise of increasing information and telecommunication security” (Maurer). The largest issue regarding cybersecurity that needs to be negotiated and addressed before progress can be made is a compliance framework. Without a compliance framework in place, any cybersecurity agreement becomes largely irrelevant, as parties can simply ignore any relevant provisions with impunity.

Topics for Consideration:
1. What activities fall under the definition of “cyberwarfare?”
2. How can any agreement regarding cybersecurity ensure compliance and good faith conduct among signatories?
3. What role, if any, do technologically advanced countries have in implementing and ensuring that cybersecurity initiatives exist in developing nations?
4. How should the current existing framework of international law apply to cyberspace?
5. What assistance, if any, can and/or should the United Nations provide to countries that are victims of cyberwarfare?

Bibliography:


Topic 4: Asymmetric Warfare in the 21st Century

1st Main Committee

The term “asymmetric warfare” is used to describe situations where great differences exist between two warring parties in military power and strategy. This contrasts with “symmetric warfare,” where the two opposing parties have comparable capabilities and success depends largely on detail and execution. To succeed in asymmetric situations, a weaker side depends on a different strategy to compensate for their power deficit. This can involve operating with greater efficiency, minimizing vulnerabilities, and employing a different form of warfare altogether. Today, asymmetric warfare often occurs in situations involving a non-state actor and a state actor. One example of this is the conflict between the Lord’s Resistance Army (LRA) and Uganda from 2005 to 2006, where the LRA, a rebel group, fought violently with the Ugandan army in northern parts of the country.

Despite cases of asymmetric warfare increasing in recent years, the current scope of international law has struggled to respond to these situations. In the example provided of the LRA and Uganda, conflict between the two sides often transcended international borders, with LRA attacks not being uncommon in the neighboring states of the Democratic Republic of the Congo and Sudan. Issues of proxy conflict, where a seemingly independent non-state actor is supported financially or technologically by a different nation, further complicates this issue. In addition, the United Nations General Assembly’s previous attempts to improve the international community’s ability to respond to asymmetric conflicts have largely focused on cases of international terrorism and have not addressed in detail the concept of state sovereignty that underlies many cases of asymmetric warfare.

To address this issue in regards to sovereignty, then United Nations Secretary General Ban Ki-Moon issued a report regarding the international community’s “responsibility to protect” (R2P) and its relationship to state sovereignty. R2P involves the international community’s ability to prevent crimes against humanity. The report proposed a three-pillared approach to R2P that states:

1. A state has a responsibility to protect its population from crimes against humanity.
2. The international community has a responsibility to assist the state to fulfill its primary responsibility.
3. If the state manifestly fails to protect its citizens from mass atrocities and peaceful measures have failed, the international community has the responsibility to intervene through coercive measures such as economic sanctions. Military intervention is considered the last resort.

In past cases of asymmetric conflict, the responsibility to follow this approach has fallen primarily on other member states, rather than a representative body of the international community such as the United Nations. This has had mixed results, as national interests can affect a state’s capacity to determine whether another state’s ability to protect its citizens is compromised. An example of this is Libya in 2011, when the members of the North Atlantic Treaty Organization, led by the United States and France, launched air strikes to remove a regime they claimed had failed to protect its citizens from the crimes outlined by the R2P. In the time afterwards, these states have met criticism that their desire for regime change was
premature and clouded by a preexisting poor relationship with Libyan leader Colonel Muammar Gaddafi.

**Topics for Consideration:**
1. What, if any, situations of asymmetric conflict fall under the responsibility of the United Nations?
2. What determines whether a state’s ability to protect its citizens is compromised?
3. Can the responsibilities to protect a particular state’s citizens be prioritized over the interests of other member states? If so, how?
4. Who should the responsibility to ascertain a state’s ability to protect its citizens from crimes outlined in R2P fall upon?
5. To what extent are cases of proxy warfare asymmetric?

**Bibliography:**


