
ILMUNC India
THE IVY LEAGUE MODEL UNITED NATIONS INDIA 2016
COSTA RICA

Dear Delegates and Faculty Advisors,

It is my distinct pleasure to welcome you to The Ivy League Model United Nations Conference India 2016 hosted by the International Affairs Association of the University of Pennsylvania, an Ivy League institution.

The Ivy League Model United Nations Conference is one of the most reputed high school conferences in the United States bringing together over 3000 delegates from across the globe in an unique academic, social and cultural experience. We are incredibly excited to bring this experience to India this year in what will be one of the largest and most academically, professionally and socially enriching Model United Nations symposiums.

Ana Rancic
Secretary-General

Jialin Zhang
Director-General

Huzefa Kapadia
President

Taylor Lewis
Chief of Staff

Alex Sands
Chief Operations Officer

Andre Na
Under-Secretary-General
Administration

A large part of what makes ILMUNC India so incredible is the commitment of its amazing staff, as well as the immense preparation that goes into making this conference the phenomenal experience that it is. Our staffers are all leaders at the prestigious University of Pennsylvania, who come from a diverse range of majors, interests, classes, and schools – from Finance at the Wharton School of Business to Computer Science and Nanotechnology at the School of Engineering. At ILMUNC India, this academic excellence and personal passions that chairs bring truly bring a professional collegiate environment and distinct enriching experience to our high school delegates, both within and outside the committee room.

The Secretariat is working hard to ensure that the quality of the conference is unparalleled. This year will bring together close to 1000 delegates in 8 distinct committees. The topics we are discussing are pertinent issues in today's world and we are excited to witness the unique and diverse solutions that our delegates will bring to the table. The ILMUNC India team is continuously searching for ways to make the conference better and more engaging for our delegates. We are proud to announce technological advancement in the Model United Nations circuit including a groundbreaking mobile application that will soon be released.

Our delegates' experiences outside of committee are just as vital as their experiences within committee. At ILMUNC India we ensure that our delegates take away memories and experiences that will better them personally and professionally. Outside of the invaluable Model United Nations experience, we host numerous college and career fairs, personal mentoring sessions with current students and alumni, keynote speeches from prominent members of society and, of course, enthralling social events.

Our delegates are the most integral part of our story and I'd like to once again thank you for choosing to be a part of our next chapter of ILMUNC India 2016. We are certain that you will walk away from this conference with memories that you will cherish for a long time to come. Welcome to ILMUNC India 2016!

Sincerely,

Ana Rancic
Secretary-General
ILMUNC India 2016

DISARMAMENT AND INTERNATIONAL SECURITY

Introduction to the Body

Formally known as "The First Committee of the General Assembly," DISEC is in charge of the establishment and maintenance of international peace and security. As the First Committee, DISEC is often tasked with solving the world's most important problems. The committee is composed of representatives from all member states of the United Nations, who are each given one vote to emphasize equality in all decisions. Its mandate, stated clearly in Article 11 of the United Nations Charter, is to "consider the general principles of cooperation in the maintenance of international peace and security, including the principles governing disarmament and the regulation of armaments."[1] DISEC discusses topics such as arms control, conflict resolution, and nuclear disarmament. Due to constantly evolving technology, however, the content discussed in committee is rapidly expanding into new topics such as cyber warfare. Unlike the Security Council (UNSC), DISEC is not allowed to impose any kind of sanctions on a nation or dictate a member's actions. Under these restrictions, DISEC constitutes a global forum that can construct internationally representative recommendations to states and other agencies, providing a concise picture of the global opinion when dealing with issues of extreme importance.

This committee will give you the opportunity to represent your country's stance and policies on the topics to be debated throughout the conference. Substantive and comprehensive resolutions are the ultimate goal of the weekend, and this background guide was created as a tool to help you begin your research on the topics at hand. In accordance with the structure of DISEC and the purview of the committee, we look forward to moderating debate on substantial and innovative solutions to these critical topics in today's global community.

Topic A: The Fifth Domain of Cyber Warfare

Statement of the Issue

Human history has long been marked with innovations in science and technology that have shaped the world. In the Middle Ages, for example, bookmaking involved copying texts and illustrations by hand. This labor intensive process, the rising costs of books, and the scarcity of education meant reading was reserved almost entirely for the clergy. In 1445, however, the introduction of Gutenberg's printing press made bookmaking exponentially more efficient. The printing press allowed for widespread ownership of books and was largely responsible for the propagation of Humanism during the Renaissance.[2]

Just as the printing press aided in the dissemination of ideas, we have entered an Information Age where the computer facilitates the

acquisition and validation of knowledge. It would not be an overstatement to say that the introduction and expansion of the Internet may be one of the most important technological revolutions in history. In just 20 years, the Internet has grown 20,000% from an estimated 16 million active users in 1995 to nearly 3.2 billion users in 2015.[3] Today, the Internet is shared between states, non-state communities, businesses, academia, and individuals. Due to the rapid rise in computer usage in both the public and private sectors, however, cyber warfare and the malicious use of the Internet has become an increasingly serious threat.

While cyberspace grows to become the "fifth" domain of warfare, questions arise as to the extent that existing international law can be transposed to the cyber domain.[4] Thus, this committee's primary objective will be to shape the cyber warfare policy of the international community.

History

The Introduction of Computers

In 1943, the United States military began work on the world's first general-purpose electronic computer. Known as the Electronic Numerical Integrator and Computer (ENIAC), the 18,000 vacuum tube machine could calculate ballistic trajectories at speeds 300,000 times faster than a human.[5] Over time, the power of computers became self-evident, growing beyond military applications to personal ones as well. The arrival of personal computers nearly thirty years later would signal the beginning of a new Information Revolution. Individuals could now own PCs with demonstrable scientific and engineering capabilities. Following Moore's Law, these computers began to shrink in physical size but grow in computing power. They still, however, were missing one defining characteristic: the ability to communicate with each other.

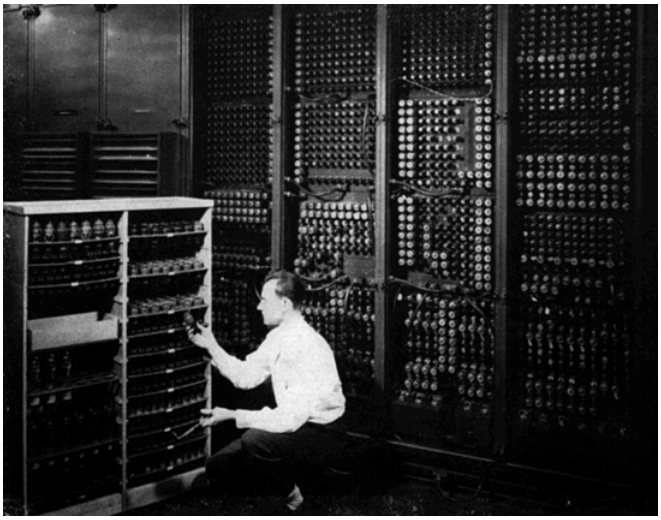

Figure 1: The world's first computer, ENIAC, consisted of nearly 18,000 vacuum tubes.[6]

The Internet

In 1962, a scientist from the United States Department of Defense's Advanced Research Projects Agency (ARPA) proposed the construction of a "galactic network" of computers that could talk to one another. Such a network would allow government officials to communicate, even if telephone systems were destroyed—a growing concern after the Soviet Union's launch of Sputnik. By 1969, the ARPANET project was complete; four computers could communicate via a method

called packet switching, in which data is broken down into blocks, or packets, before being sent to its final destination. As more networks were added, however, it became difficult to integrate them into a single worldwide Internet.

In 1991, Tim Berners-Lee built off thirty years of past Internet research to transform the internet into a worldwide network. He introduced the World Wide Web: an internet that was not simply used to send files from one place to another, but was itself a "web" of information that anyone could access.[7]

The Rise of Malicious Code

The strength of the Internet lied clearly in its connectivity. It enabled users to discover and disseminate information in near real-time, to communicate quickly and privately, and to store a wealth of personal information. Unfortunately, these benefits also made it vulnerable to novel, large-scale attacks and susceptible to swift, massive damage. As Internet connectivity grew, malicious users were able to conduct increasingly asymmetric attacks. In theory, an attacker could target all internet-connected computers simultaneously.[8]

Examples of computer viruses occurred as early as 1971, when the Creeper worm affected the ARPANET project. While this worm did not attempt to steal or destroy data, it gave rise to the notion of malicious code.[9] Then in 1988, the Morris worm became the first recognized malicious worm to affect the world's nascent cyber infrastructure.[10] Since 1988 an influx of cyber attacks have affected states, non-state communities, businesses, and individuals[11]:

- April 2007 – Estonian government networks were harassed by a denial of service attack by unknown foreign intruders, following the country's political confrontation with Russia over the removal of a war memorial commemorating Soviet conquest of Estonia during WWII. Some government online services were temporarily disrupted and online banking was halted.
- October 2007 – China's Ministry of State Security said that foreign hackers, which it claimed 42% came from Taiwan and 25% from the United States, had been stealing information from Chinese key areas.
- August 2008 – Computer networks in Georgia were hacked by unknown foreign intruders around the time that the country was in conflict with Russia. Graffiti appeared on Georgian government websites. There was little disruption of services but the hacks did put political pressure on the Georgian government and appeared to be coordinated with Russian military actions.
- January 2010 – A group named the "Iranian Cyber Army" disrupted the service of the popular Chinese search engine Baidu. Users were redirected to a page showing an Iranian political message.
- October 2010 – Stuxnet, a complex piece of malware designed to interfere with Siemens industrial control systems, was discovered

in Iran, Indonesia, and elsewhere, leading to speculation that it was a government cyber weapon aimed at the Iranian nuclear programme.

- January 2011 – The Canadian government reported a major cyber attack against its agencies, including Defence Research and Development Canada, a research agency for Canada's Department of National Defence. The attack forced the Finance Department and Treasury Board, Canada's main economic agencies, to disconnect from the Internet.
- October 2012 – The Russian firm Kaspersky discovered a worldwide cyber-attack dubbed "Red October," that had been operating since at least 2007. The virus collected information from government embassies, research firms, military installations, energy providers, nuclear and other critical infrastructures.

Figure 2: "Iranian President Mahmoud Ahmadinejad observes computer monitors at the Natanz uranium enrichment plant in central Iran, where Stuxnet was believed to have infected PCs and damaged centrifuges."[12]

Cyber Armies

In 1993, a United States Naval Postgraduate School (NPS) article examined the historical aspects of "cyberwar," in which its authors argue "the Information Revolution would change not only how wars are fought, but even why wars are fought."[13] Cyberwar to the 21st century could be analogous to what blitzkrieg was to the 20th century: a means for turning the balance of information in one's favor, even if the balance of conventional force is not.

In 2001, James Adams revealed in Foreign Affairs that the United States Department of Defense had put cyberwar theories to real-world tests in a classified 1997 exercise codenamed "Eligible Receiver." In the tests, thirty-five U.S. National Security Agency personnel impersonated North Korean hackers and used a variety of tactics to successfully attack the U.S. Navy's Pacific Command from cyberspace.[14]

Almost a decade later, a 2009 report on the People's Republic of China's cyber warfare capabilities indicated that the country constructed a "highly-networked force that... has a clear, offensive cyber mission in times of both war and peace."[15] In times of peace, cyber espionage will gather strategic intelligence to help win future wars. In times of war, a range of computer network operations and electronic warfare tactics will be used to achieve information superiority over an adversary.[16]

In order to combat these growing instances

of cyber warfare, actions are being taken on both a national and international scale.

Relevant International Action

Scientists began to warn the world about the danger of computer hacking shortly after World War II.[17] Since then, the cyber world has been in significant flux; the magnitude of cyber security is clear, but agreements on even the most basic underlying definitions are still being reached.

In the last several decades, norms surrounding cyber security have begun to emerge in the United Nations. The norm emergence process can be divided into two main streams of negotiations: "politico-military" issues and "economic" issues.[18] The politico-military stream is concerned with how "[information] technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States."[19] The economic stream, on the other hand, is about "the criminal misuse of information technologies."[20] For the purposes of this committee, the focus will be on the politico-military stream, which can alternatively be defined as cyber warfare.

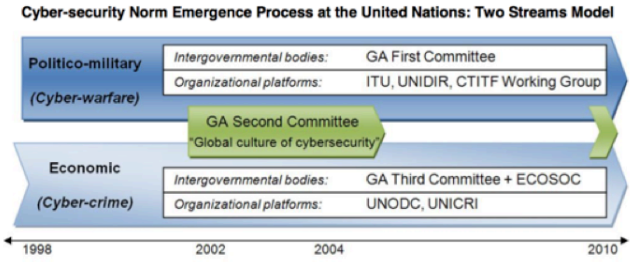

Figure 3: UN governing bodies broken down by the two streams of norm emergence, politico-military and economic.[21]

Other Organizational Platforms

The United Nations Institute for Disarmament Research (UNIDIR)

UNIDIR in Geneva was one of the first UN bodies to become involved in cyber security. The body has recently published a research project titled "Perspectives on Cyber War: Legal Frameworks and Transparency and Confidence-Building". The intended goal for the project was to raise awareness "among diplomats and policymakers about the specter of cyber war and to begin multilateral discussions about how to prevent and restrain such conflicts."[22] In addition, UNIDIR has held several conferences relating to discussions that have taken place in the First Committee.

The International Telecommunication Union (ITU)

The ITU "is the United Nations organization that has most responsibility for practical aspects of cyber security."[23] It serves as the only treaty

organization in the UN that deals with issues related to cyber security and cyber warfare. Since it joined the UN system under Article 57 of the UN Charter, it has played an important role in setting technical standards for the international community. The ITU also provides experts as a resource base in the event of a cyber attack. The Secretary-General of the ITU submits a quarterly assessment of cyber threats to the Secretary-General of the UN, and shepherds the Global Cybersecurity Agenda.[24]

The Counter-Terrorism Implementation Task Force (CTITF)

The United Nations Secretary-General created the CTITF in 2005 to strengthen coordination and coherence of counter-terrorism efforts of the United Nations system. CTITF organizes its work through Working Groups, one of which being the "Protection Of Critical Infrastructure Including Internet, Vulnerable Targets And Tourism Security." While cyber terrorism is not directly comparable to cyber warfare, it is useful proxy for recommendations that can be made to member states to improve cyber security and decrease the threat of cyber warfare.[25]

Figure 5: A meeting of the CTITF at the United Nations.[26]

Current Situation

Since 2011, cyber warfare has remained a major concern in the international community. While many countries recognize the threat of cyber war, efforts to internationally sanction cyber war have come up short. Instead, countries are rapidly building defensive cyber mechanisms to protect against targeted attacks. Moreover, certain technology-advanced countries have been exceedingly willing to accuse other nations of their use of cyber weapons, while simultaneously developing offensive cyber capabilities of their own. This turbulent, finger-pointing climate and the growing signs that cyber warfare promises military, economic, and strategic advantage over other nation-states, signals what many view to be the start of a cyber arms race. Thus, the goal for this First Committee is to focus on and address the following important areas facing the international community today.

Cyber Warfare vs. Common Warfare

Presently, cyber warfare is defined as "warfare conducted in cyberspace through cyber means and methods."[27] Warfare, however, is often thought of as the conduct of military hostilities in situations of armed conflict. This creates difficulties in applying existing international law to cyber warfare, due to special considerations that come into play with cyberspace.

First, cyberspace is not geopolitically or naturally bound. Especially today—when it is easy to disguise the origin of an operation with IP spoofing and the use of botnets—reliably identifying

and attributing cyber activities to a nation, non-state actor, enterprise, or individual is particularly difficult.

Second, according to article 2(4) of the UN Charter, "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[28] The question thus arises as to what extent cyber warfare should be considered an internationally wrongful threat or use of force. In fact, cyber operations almost always fall within the grey area between traditional military force and other forms of coercion, and were simply not anticipated by the drafters of the UN Charter.[29]

Third, it is difficult to apply the conventional idea of civilian casualties to acts of cyber war. Often in acts of kinetic war, the principle of "proportionality" comes into play when determining lawfulness in jus in bello of any armed attack that causes civilian casualties. Simply put, attacks are prohibited if they cause incidental loss of civilian life that is excessive in relation to the anticipated military advantage of the attack. Thus, the First Committee should consider alternatives to determining proportionality in acts of cyber war, where there is little direct infliction of death, injury, or destruction. One way, for example, could be a consideration of damage done on "critical infrastructures," as defined by the United Nations General Assembly as:

"those used for, inter alia, the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health—and the critical information infrastructures that increasingly interconnect and affect their operations."[30]

State Versus Non-state Actors

Article 2(4) of the UN Charter is addressed to states only; thus, persons or parties not acting with the permission of a state government cannot be regarded as state agents and can instead be described as "non-state actors." In cyberspace, acts of cyber war by non-state actors pose a significant threat, given the lower barriers of entry to cyber warfare. The resources needed to engage in this particular act of war are far less significant than the resources need to engage in kinetic warfare. In fact, experts are increasingly concerned as cyber warfare moves towards an army of one—only one individual could pose significant threat to a nation's critical infrastructure. Dealing with these non-state actors will be one of the greatest challenges facing this committee and the international community as a whole, as "the use of force (including through cyber operations) by individual hackers and other non-state actors may be relevant under international humanitarian law and, in some cases, international criminal law, but is not prohibited by article 2(4) of the UN Charter."[31]

Analysis

Developments in Telecommunication Law

The Russian Federation first introduced a

draft resolution on "Developments in the field of information and telecommunications in the context of security" to the First Committee in 1998. Russia hoped to "develop international law regimes for preventing the use of information technologies for purposes incompatible with missions of ensuring international stability and security."[32] Since then, interaction in the First Committee has been primarily between the Russian Federation and the United States. The Russian Federation has called for a cyber arms control treaty, while the United States has adopted a position that "the same laws that apply to the use of kinetic weapons should apply to state behavior in cyberspace."[33]

Phase 1: 1998-2004

In the 1998 draft resolution, the Russian Federation introduced an "international computer security treaty" that built off previous work in Resolution A/53/576, "Role of science and technology in the context of security, disarmament and other related fields." The key elements of this treaty were as follows. First, the treaty mentioned the military potential for information technology and, for the first time, expressed concern over its potential to be used for reasons inconsistent with the stability and security of States. Second, the draft resolution mentioned the need to prevent cybercrime and cyberterrorism. Finally, it encouraged member states to inform the Secretary-General of their views and positions on "definitions" and the development of "international principle."[34] The draft resolution was later adopted by the General Assembly without a vote in January 1999 as Resolution 53/70.

Although the draft resolution was adopted, many countries were skeptical about the push for an international treaty. Their concern was that such a treaty could limit individuals' access to and freedom of information under the pretense of increasing information technology security.[35] At the same time, however, many recognized the United States' incentive not to limit the use of such technologies, given that it was the clear leader in information security.

Phase 2: 2005-2008

The period from 2005 to 2008 was critical for cyber security and cyber warfare. It marked some of the first signs of regression and contentious debate in the First Committee.

In 2004 the first Group of Governmental Experts (GGE) was established to present a report on cyber security to the Member States of the United Nations. The Group was comprised of experts from fifteen States: Belarus, Brazil, China, France, Germany, India, Jordan, Malaysia, Mali, Mexico, the Republic of Korea, the Russian Federation, South Africa, the United Kingdom of Great Britain and Northern Ireland, and the United States of America. When it came time to present the report in 2005, however, the GGE failed to come to a common position. "Given the complexity of the issues involved, no consensus was reached on the preparation of a final report," said Secretary-General Kofi Annan.[36] This outcome was quite unusual for any United Nations GGE,

which are typically only formed when it is clear that the countries involved can agree on some smallest denominator in the event that no other agreements are reached.

This failure to reach consensus indicated the growing uncertainties surrounding cyber security in the United Nations. According to A.A. Streltsov, a member of the Russian Federation delegation at the GGE meetings, "The main stumbling block was the question of whether international humanitarian law and international law sufficiently regulate the security aspects of international relations in cases of 'hostile' use of ICTs for politico military purposes. However, the work of the GGE was not in vain. It successfully raised the profile of the relevant issues on the international agenda."[37]

In addition to the failure of the GGE in 2005, draft resolutions in the First Committee during this period highlight the dynamic progress the United Nations was making on the issue of cyber warfare. In 2005, a draft resolution introduced by the Russian Federation went to a vote for the first time in history. While the draft resolution was ultimately adopted, one country voted against the resolution: the United States.[38] After the United States voted in opposition of the 2005 draft resolution, it set the stage for multilateral sponsorship of resolutions. When the next draft resolution was introduced in 2006 it was co-sponsored by the Russian Federation, the People's Republic of China, Armenia, Belarus, Kazakhstan, Kyrgyzstan, Myanmar, Tajikistan, and Uzbekistan.[39]

Phase 3: 2009-2011

Beginning in October 2009, draft resolutions in the First Committee were adopted without a vote—as they were before 2005.[40] This period from 2009 to 2011 marked significant progress in agreements on cyber warfare policy in the United Nations. In 2010, the United States presented a position paper that helped bring parties closer together. Later that year, the second GGE was able to reach a consensus and publish a conclusion in its report.[41] Overall, the GGE found that, "Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century."[42] The Group identified both potential perpetrators and potential victims, declared the risk that cyber warfare has to "international peace and national security," and provided five recommendations to create a "global culture of cyber security":

1. Further dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructures;
2. Confidence-building, stability, and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict;
3. Information exchanges on national legislation, national ICT security strategies and technologies, policies and best practices;
4. Identification of measures to support capacity-building in less developed countries;

5. Finding possibilities to elaborate common terms and definitions relevant to United Nations General Assembly resolution 64/25[43]

During this time period the United States also decided to co-sponsor the Russian Federation's draft resolution in the First Committee. For the first time in history, the U.S. would join three dozen other countries, including the People's Republic of China, as a co-sponsor of Resolution 65/41. This willingness to cooperate further signaled the "increased understanding of the international need to address the risk [of cyber warfare]."[44]

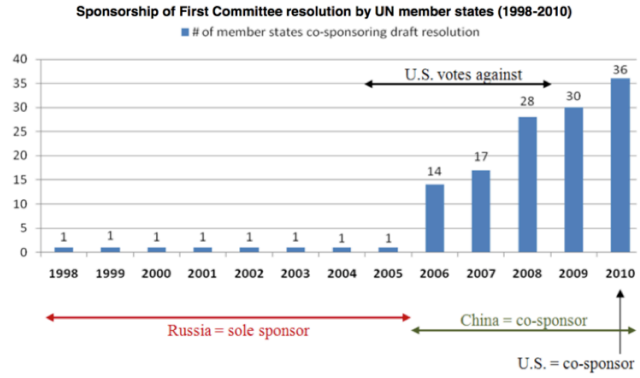

Figure 4: Chart indicating the number of member states co-sponsoring draft resolutions over time.[45]

Possible Solutions

As this First Committee works towards solutions for governing cyber warfare, delegates should, at a minimum, consider the following two different possible approaches.

Applying Existing Laws for Warfare to Cyberspace

While cyberspace itself imposes a fifth domain of warfare, it may be practical in many instances to apply existing laws that govern kinetic warfare to cyber warfare. Delegates pursuing this as a possible solution must bear in mind the aforementioned limitations of such laws and consider revisions that can be made to better apply to cyber warfare. For example, delegates should redefine the principle of proportionality as it applies to cyber warfare. Delegates must also determine new methods for protecting against and punishing non-state actors.

New Methods of Governing Cyber Warfare

Yet another possible solution this First Committee could pursue is defining entirely new methods of governing cyber warfare. Some experts have suggested that new treaties may "provide a better framework for establishing definitions for cyber aggression."[46] Many of these treaties are outlined in "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," a 2009 paper by Scott Shackleford. He suggests drawing on several existing treaties to construct an international cyber treaty:

- Nuclear nonproliferation treaties
- The Antarctic Treaty System and Space law
- United Nations Convention on the Law of the Sea (UNCLOS)
- Mutual Legal Assistance Treaties (MLAT)[47]

Figure 6: First session of the Legal Committee on Peaceful Uses of Outer Space.[48]

Bloc Positions

In 2007, Internet security company McAfee reported that 120 countries had engaged in launching cyber espionage operations. With cyber warfare still in nascent stages, however, many countries have yet to take concrete positions on the issue. Furthermore, traditional blocs and alliances have not necessarily applied. The United States and Europe have expressed concern with China's cyber aggression, yet many European countries have varied their willingness to support the United States and Israel's Stuxnet efforts to disrupt Iranian nuclear development. The unclear and often contradictory positions of many countries have only been exacerbated by certain countries' lack of cyber capabilities. Many of these countries act as bystanders in debate - lacking both offensive and defensive capabilities but understanding the reality of the increasingly digital and vulnerable world. Given the lack of traditional blocs in this situation, countries can best be categorized as follows:

Countries with Offensive Cyber Capabilities

While many countries have understood the importance of cyber capabilities, certain countries have spent decades developing both strong offensive and defensive mechanisms. Among the most prominent of these countries is the People's Republic of China, whose relatively limited traditional military capacity has led to aggressive advancement of cyber weaponry.[49] The Chinese government uses "new space-based surveillance and intelligence gathering systems" to support its "informationization" strategy, which includes "increased education of soldiers in cyber warfare [and] a reorganization of military branches and command system."[50] As aforementioned, the Russian Federation also falls into this category of countries with both offensive and defensive cyber capabilities. Other countries that fall into this category include Iran—who "is considered an emerging military power in the field of cyber warfare"[51] —and North Korea. The United States and Israel also fall into this category, as both of them have advanced offensive cyber technologies. Though hesitant to employ offensive measures (as to avoid a cyber arms race), both countries have shown willingness to operate covertly when it pertains to self-identified, highly pressing threats.[52]

Figure 7: U.S. sailors assigned to Navy Cyber Defense Operations Command take their stations.[53]

Countries Wishing to Limit Cyber Capabilities

Most countries that fit into this category have built some elements of cyber weaponry or espionage. Several countries, such as Japan and Germany, even have rather strong cyber capabilities.[54] Countries in this category, however, do not want to engage in, provoke, or open a new arena of cyber combat, due to the immense amount of resources required to compete at the highest level. Especially in times of economic distress and budget regulations, these countries have attempted to limit development of offensive cyber infrastructure at the international stage, and have often supported defensive measures to build deterrent capabilities against China and North Korea. This category includes most European countries and several countries in Asia.[55]

Countries with Limited Cyber Capabilities

While nearly all countries understand the risks of cyber warfare, some countries already have very limited cyber defense mechanisms. These countries worry that cyber weapons could be disastrous for military, financial, and public systems. Furthermore, they see cyber warfare as yet another means for more powerful countries to exploit weaker ones. As such, these countries frequently oppose development of cyber capabilities, instead favoring new laws that limit or ban cyber warfare.

A Focus on Cyber Monitoring

Additionally, there is a subset of countries that, as a result of their limited cyber capabilities, have shifted their focus from cyber warfare to cyber monitoring. This is especially prevalent in countries experiencing civil unrest and political volatility. Countries in this category, such as Eritrea, Turkey, Malaysia, Thailand, and Egypt, seek to ensure that any new international laws on cyber warfare do not affect governments' ability to monitor and regulate the Internet.[56]

Preventing Cyber Crime

Finally, there is another set of countries in this category that have been more concerned with cyber crime. It's not to say, however, that these countries are not concerned with the rise of cyber warfare. But given the weaker underlying cyber capabilities, countries in this bloc—mostly African nations—have become targets for recent cyber crimes with major economic impacts. In Kenya, for example, a recent report says that businesses are losing about

$146 million every year to cyber crime.[57] Similarly, in South Africa, a newspaper reported that "hackers launched 6,000 cyber-attacks against South African infrastructure, internet service providers (ISPs), and businesses in October alone."[58] As such, these countries are concerned mostly with laws surrounding the sovereignty of pursuing cyber criminals.

Questions a Resolution Must Answer

1. How should the United Nations define cyber war? How will traditional definitions as an act of "force" change with this new fifth domain of warfare?
2. Should cyber war be banned, or is this the inevitable future domain of warfare?
3. What existing laws or treaties can be applied to govern acts of cyber war? What mechanisms can be put in place to prevent a cyber arms race?
4. How can the non-governmental actors be punished for acts of cyber war? How will state actors defend against increasingly mobile, non-state "armies of one"?
5. Do countries with offensive cyber capabilities and significant resources have a responsibility to contribute to the cyber security of other countries? How will countries with limited cyber capabilities protect against acts of cyber war, if not?
6. Issues of Internet privacy may prevent countries from monitoring potential acts of cyber war. To what extent should states be able to monitor actions taken in cyberspace that may infringe on civilian privacy?

Conclusion

Many experts have claimed cyberspace to be the "fifth" domain of warfare.[59] As the Internet continues to grow at unprecedented rates, its expansion poses threats to security for member states of the United Nations. With today's Internet being shared between states, non-state communities, businesses, academia, and individuals, it serves as an obvious target for attack. Traditional acts of kinetic war, however, do not compare well with operations carried out in cyberspace. As such, existing laws and treaties governing acts of international force need to be rethought. It will be this primary objective that guides the First Committee of the General Assembly.

Topic B: Nuclear Policy for the 21st Century

Statement of the Issue

Statement of the Issue

The evolution of nuclear policy in the past century has distinctly marked the order of the international community, bringing new safety and security concerns onto the world stage like no other weapons development ever has. While the Cold War has ended, the advances in technology related to nuclear weapons pose significant problems for the global community today. While there has been no conflict of comparable scale to the rising escalation of Cold War tensions in the past, the international

community today, due to technological innovation of communication, transportation, and weaponry, faces new challenges regarding nuclear policy in the 21st century.

Stephen M. Younger, the Associate Laboratory Director for Nuclear Weapons at the Los Alamos National Laboratory in the United States, has analyzed the correlation between the technological innovations in the composition of nuclear forces with the changing policy for their use in the 21st century significantly. He notes that with the changes in geopolitical relations that have marked the 21st century so far, "the time is right for a fundamental rethinking of our expectations and requirements for these unique weapons."[60] He goes on further to elaborate that such composition of nuclear arsenals around the world have the flexible ability to undergo rapid and significant modification to respond to "changing conditions, changing military needs, and changes in our confidence in our ability to maintain credible nuclear forces without nuclear testing or large-scale weapons production."[61] It is the rapid ability to alter the purposes of a nuclear arsenal that leave nuclear policy in the 21st century a key subject of international skepticism and debate.

Nuclear energy, as it continues to become a form of sustainable energy security, will play a significant role in the climate change debate and the movement to lower dependency on fossil fuels. As the Director General of the International Atomic Energy Agency Yukiya Amano has cautioned, "it will be difficult for the world to achieve the twin goals of ensuring sustainable energy supplies and curbing greenhouse gases without nuclear power."[62] This committee's primary purpose will be to shape the nuclear policy of the international community today. The committee must find balance between the need for sustainable energy and the threat that nuclear weapons and their advancing technologies pose to the global community. The three crucial areas of nuclear policy, nuclear disarmament, nuclear energy, and nuclear non-proliferation, will play a central role in understanding the objectives and limitations of any nuclear policy plan in the 21st century.

Figure 8: A Nuclear Power Plant in Tennessee, United States. Nuclear power remains a significant source of reliable non-greenhouse-gas emitting electric power in the United States and other countries.[63]

History

A brief overview of the development of nuclear policy in the international community is as follows:

- 1895-1945: Focus centered on the science behind atomic radiation, atomic change, and nuclear fission is researched and developed,

with the most significant advances taking place from 1939-1945.

- 1939-45: Focus is given to the construction of an atomic bomb.
- 1945: Focus shifts towards harnessing nuclear power for energy.
- 1956-Present: Focus continues to be centered on creating sustainable nuclear power plants.[64]

Early Scientific Innovation

The development of nuclear weapons over the past century has been built upon centuries of scientific exploration and discovery regarding the power of the atom. The discovery of uranium in 1789 by Martin Klaproth marked the beginning of scientific experimentation with radioactivity and eventually with nuclear fission.[65] The subsequent quests for innovation regarding nuclear energy and nuclear weapons would go on to dominate the scientific arena for the following two centuries. From 1789 until 1938, continual discovery regarding ionization and radioactivity was conducted.[66]

At the end of 1938 Otto Hahn and Fritz Strassmann in Berlin "showed that the new lighter elements were barium and others which were about half the mass of uranium, thereby demonstrating that atomic fission had occurred."[67] At the same time, Lise Meitner and her nephew Otto Frisch, working under Niels Bohr, were able to explain this phenomenon by suggesting "the neutron was captured by the nucleus, causing severe vibration leading to the nucleus splitting into two not quite equal parts."[68] This scientific discovery prompted further research in laboratories across the world. Francis Perrin, in 1939, was able to determine the remaining piece of the puzzle that had not yet been discovered. He introduced the "concept of the critical mass of uranium required to produce a self-sustaining release of energy."[69]

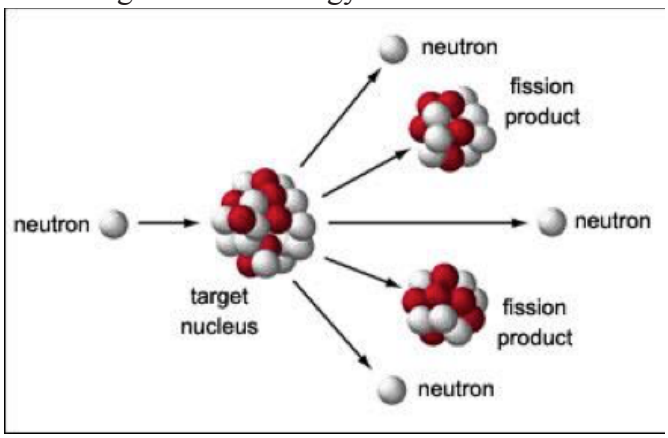

Figure 9: The figure above depicts the theory of atomic fission and the energy released in such fission.[70]

World War II

After the Japanese bombing of Pearl Harbor on December 7, 1941, the United States entered World War II, marking a new phase of development in nuclear policy. After US entry into the War, the "Manhattan Project" came into development, combining key scientists and research facilities across the United States under the War Department's effort to develop an atomic bomb.[71] By 1943, the United States had established a combined policy committee with Great Britain and Canada. Scientists from those countries then moved to the United States to join the project there.[72]

The first atomic bomb exploded on July 16, 1945 in New Mexico. The following month, two other atomic bombs produced by the project, "the first using uranium-235 and the second using plutonium"[73], were dropped on Hiroshima and Nagasaki, Japan.

Figure 10: The atomic bomb dropped in Nagasaki, Japan was responsible for the immediate death of 42,000 individuals and the injury to 40,000 additional individuals. The bomb destructed 39% of all standing buildings in Nagasaki.[74]

At the same time, nuclear research in Germany and the Soviet Union had been taking place. With the conclusion of World War II and the defeat of Nazi Germany by May of 1945, "German scientists were 'recruited' to the bomb program to work in particular on isotope separation to produce enriched uranium. This included research into gas centrifuge technology in addition to the three other enrichment technologies."[75]

Cold War

Post-war, weapons development continued on both sides of the "iron curtain", but a new focus was on harnessing the great atomic power, now for the purpose of making steam and electricity. In the course of developing nuclear weapons the Soviet Union and the West had acquired a range of new technologies and scientists realized that the process could be utilized either directly or for generating electricity. It was also clear that this new form of energy would allow development of compact long-lasting power sources that could have various applications.[76]

Accidents

There have been a number of accidents resulting from the mismanagement of nuclear facilities throughout history. The most important of these accidents are the SL-1 Accident, the Three Mile Island Accident, Chernobyl, and Fukushima Daiichi. The SL-1 Accident took place in January 1961 at the National Reactor Testing Station in Idaho, and was the result of an overheated rod which ultimately caused an explosion. The explosion caused the immediate death of one reactor employee, and resulted in radiation exposure to more than twenty individuals.[77] The Three Mile Island incident took place in March of 1979 in Pennsylvania. The plant's reactor melted down, and highlights the most serious incident of nuclear safety mismanagement in commercial nuclear power history.[78] The nuclear incident at Chernobyl, which took place in April of 1986, was the result of a flawed Soviet nuclear reactor design. The accident ultimately led to an explosion and subsequent fire

in Chernobyl, Ukraine. Acute radiation poisoning was a major result of Chernobyl, and the accident there led to major changes in safety culture and in industry cooperation."[79] The most recent nuclear accident took place in Japan in March 2011, and was initially caused by the resulting tsunami after the Tohoku Earthquake. The cores of three nuclear reactors there melted as a result of the tsunami. While there were no immediate deaths from exposure to radiation, more than 100,000 people were evacuated from their homes in efforts to minimize radiation exposure.[80] The situation in Japan reflects the most modern accident of commercial nuclear energy and the increasing difficulty with expanding population sizes to ensure reliable energy while protecting human lives. Ultimately, it becomes clear that as the international community watches the 21st century unfold, there are new prospects at play for the crucial need to develop nuclear power. These include the "realization of the scale of projected increased electricity demand worldwide […] [the] awareness of the importance of energy security, and [...] the need to limit carbon emissions due to concern about global warming."[81]

Relevant International Action

There has been a wide array of action taken regarding nuclear policy, nuclear energy, nuclear weapons, and the correlation of the three in the past decades. Notably, the United Nations has played a crucial role in halting the spread of nuclear arms and has created relevant bodies to deal directly with nuclear policy in the global community. The International Atomic Energy Agency (IAEA) has most notably responded to the global community's development as a nuclear world.

The International Atomic Energy Agency, also referred to as the "Atoms for Peace" organization, was created in 1957 to help respond to the growing fears and anxieties about the mounting nuclear arms race. While the IAEA was established outside of the United Nations through its own statute, the body reports to the United Nations Security Council as well as the United Nations General Assembly. The IAEA's main purpose is to work for "the safe, secure and peaceful uses of nuclear science and technology."[82] Its three main missions include peaceful uses, safeguards, and nuclear safety standards. In striving for these three missions, the IAEA seeks to "assists its Member States, in the context of social and economic goals, in planning for and using nuclear science and technology for various peaceful purposes, including the generation of electricity, and facilitates the transfer of such technology and knowledge in a sustainable manner to developing Member States."[83] Additionally, the IAEA seeks to help develop and maintain various nuclear standards for safety and regulation while promoting "the achievement and maintenance of high levels of safety in applications of nuclear energy, as well as the protection of human health and the environment against ionizing radiation."[84] Lastly, the IAEA, through verification and inspection systems, ensures that States "comply with their commitments, under the Non-Proliferation Treaty

and other non-proliferation agreements, to use nuclear material and facilities only for peaceful purposes."[85] The IAEA currently has 168 members.

Figure 11: The IAEA headquarters are based in Vienna, Austria.[87]

The IAEA has been responsible for the successful fruition of a plethora of treaties regarding nuclear regulation and monitoring in the international community. Below is a list of treaties under IAEA's jurisdiction:

- Convention on Early Notification of a Nuclear Accident (adopted September 1986)
- Convention on Assistance in the case of a Nuclear Accident or Radiological Emergency (adopted September 1986, entered into force October 1986, entered into force February 1987)
- Convention on Nuclear Safety (adopted June 1994, adopted October 1996)
- Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management (adopted September 1997, entered into force June 2001)
- Convention on the Physical Protection of Nuclear Material (adopted October 1979, entered into force February 1987)
- Amendment to the Convention on the Physical Protection of Nuclear Material (entered into force May 2016)
- Vienna Convention on Civil Liability for Nuclear Damage (adopted May 1963, entered into force November 1977)
- Joint Protocol Relating to the Application of the Vienna Convention and of the Paris Convention (adopted September 1988, entered into force April 1992)
- Protocol to Amend the Vienna Convention on Civil Liability for Nuclear Damage (adopted September 1977)
- Convention on Supplementary Compensation for Nuclear Damage (adopted September 1997)

Current Situation

The United Nations Office for Disarmament Affairs was established in January of 1998 in efforts to promote nuclear disarmament and nonproliferation, promote disarmament attempts in the "area of conventional weapons, especially landmines and small arms, which are the weapons of choice in contemporary conflicts,"[88] and strengthen the disarmament regimes "in respect to other weapons of mass destruction, and chemical and biological weapons."[89]

The most recent international forum to discuss the role of nuclear power in the 21st century took

place in June of 2013 in Saint Petersburg, Russian Federation. There, leaders from the international community gathered to discuss the role of nuclear power in contributing to sustainable development while also examining the safeguards necessary to ensure nuclear safety and other prerequisites for nuclear power. Because several countries are planning to introduce nuclear power within their borders in the near future, the Conference heavily focused on the necessary preparative steps of developing nuclear infrastructure and managing radioactive waste. "The Conference [also] discussed[ed] how governments and other investors [could] create conditions that foster the deployment of innovative technologies, such as fast reactors, closed fuel cycles and new designs of small modular reactors."[90]

Nuclear policy has been the focus of the international community and many UN organs for decades. Correlating to the history of the development of nuclear weapons, a number of multilateral treaties have been created with the goal of deterring nuclear proliferation and other nuclear testing. These treaties seek to promote nuclear disarmament. The primary treaties that have been drafted and signed into action to date include the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), the Treaty Banning Nuclear Weapon Tests In The Atmosphere, In Outer Space And Under Water (known as the Partial Test Ban Treaty (PTBT)), and the Comprehensive Nuclear-Test-Ban Treaty (CTBT). The CTBT is the only treaty which has been signed (1996) but which has still yet to enter into force.[91] The most significant of these treaties, the NPT, was opened to signature in June 1968 and was ratified into force in March of 1970. This treaty pertains to "the obligation to prevent the spread of nuclear weapons and weapons technology, to promote cooperation in the peaceful uses of nuclear energy and to further the goal of achieving nuclear disarmament and general and complete disarmament."[92]

Analysis

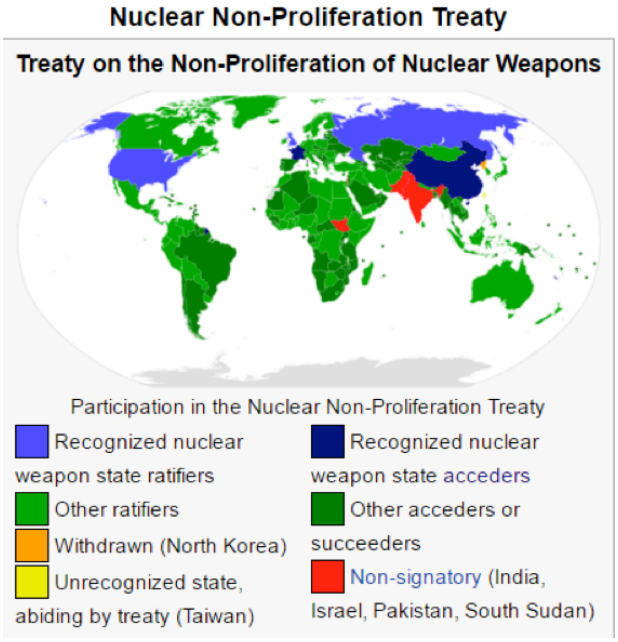

Figure 12: A map of the global world order and a breakdown of states' recognition of NPT.[93]

There are also many bilateral/multilateral agreements and other international arrangements that aim to "reduce or eliminate certain categories of nuclear weapons, to prevent the proliferation of such weapons and their delivery vehicles."[94] The agreements between the United States and Russian

Federation are a primary example of such bilateral agreements. From 1969 to the present day, the United States and Russian Federation have engaged in bilateral agreements in order to control the size of nuclear arms arsenals in the country. SALT I, SALT II, START I, START II, SORT, and New START are all bilateral agreements between the countries that have been created with intentions to slow the pace of the buildup of nuclear arms by each country.[95] Other arrangements include initiatives to the Nuclear Suppliers Group, the Missile Technology Control Regime, the Wassenaar Arrangement, and the Hague Code of Conduct against Ballistic Missile Proliferation.[96]

The most notable international action to date is United Nations Security Council Resolution 1540, adopted unanimously in April of 2004. The resolution "imposes binding obligations on all States to adopt legislation to prevent the proliferation of nuclear, chemical and biological weapons, and their means of delivery, and establish appropriate domestic controls over related materials to prevent their illicit trafficking. It also encourages enhanced international cooperation on such efforts."[97] In 2006, 2008, 2011, the Security Council has adopted subsequent resolutions, 1673, 1810 and 1977 respectively, to extend the mandate of the 1540 Committee until 2021.

Today, the current situation regarding nuclear policy is heavily influenced by both international organizations and individual states. The IAEA specifically has spearheaded a variety of initiatives regarding the various facets of nuclear use, with the aim to partner directly with member states and advance the application of nuclear technology in a wide array of fields. These fields include health, food, industrial output, agriculture, and water resources.[98]

There has also been tremendous progress in the monitoring of nuclear capabilities and their scientific contributions towards the improvement of human health, water resources, and other marine and land environments as a result of IAEA oversight.[99] This nuclear safety and security has advanced globally in large part due to the creation of the Global Nuclear Safety and Security Framework (GNSSF). This framework serves as an effective logistical gateway to safety and security standards and methods, effectively creating the ability to "achieve and maintain worldwide a high level of safety and security at nuclear facilities and activities."[100]

The international community has also taken action to establish various nuclear-weapon-free zones. These zones, while first established in the 1967 Treaty of Tlatelolco, have continued to be established through the modern day. The 2006 Treaty of Semipalatinsk marked another leap forward for nuclear-weapon-free zones, with talk of the creation of new zones in the Arctic and the Middle East continuing today.[101] Furthermore, "progress with current NWFZs is also being made—the protocols to the Treaty of Pelindaba were submitted to the

US Senate in May 2011 for consent to ratification, making the United States the final nuclear-weapon state to do so."[102] To date, the only countries with nuclear weapons are the United States, Russian Federation, United Kingdom, China, France, India, Pakistan, Israel, and North Korea. These nine countries together possess more than 15,000 nuclear weapons. The United States and Russia maintain roughly 1,800 of their nuclear weapons on high-alert status – ready to be launched within minutes.[103] The growth of nuclear weapons states will remain a concern for the international community moving into the 21st century. These nuclear-weapon-free areas, however, provide a template for international cooperation and regional support in preventing the spread of nuclear weapons states in the global order.

Figure 13: A map of nuclear-weapon-free areas in the international community, created to help strengthen global non-proliferation.[104]

Possible Solutions

Nuclear energy will undoubtedly continue to play an important role as one of the world's most prominent and efficient non-greenhouse-gas-emitting energy sources. Thus, within this committee, delegates will need to find a way to balance the benefits of nuclear energy with the negatives, as well as mitigate potential use of nuclear weapons by terrorist groups and as a source of weaponry in the modern day. As the committee focuses on drafting implemental nuclear policy for the twenty-first century, many areas of nuclear policy will need to be addressed. These areas include, but are not limited to, nuclear waste management, the use of nuclear energy, prevention of the acquisition of nuclear weapons by terrorist groups, nuclear non-proliferation globally, and a reduction in nuclear arms from countries with nuclear capabilities. Ultimately, delegates will be responsible not only for representing their country's nuclear policy, but for envisioning a feasible nuclear policy that can be implemented on a global scale to deal with growing concerns regarding nuclear energy in the modern day.

The resolutions that this committee will draft must focus on the variety of issues connected to nuclear policy in the 21st century. These primary issues, amongst others, include nuclear disarmament, nuclear energy, and nuclear non-proliferation.

Bloc Positions

Listed below are some of the most important or unique nuclear policy positions in the 21st century. These positions represent various schools of thought regarding nuclear energy, nuclear weapons, and the progression of nuclear policy into the 21st century and beyond.

The United States of America

The United States remains committed to maintaining a nuclear arsenal that is capable of serving as a deterrent against attack. The United States has, however, expanded the Department of Defense's scope to include a large increase in the production of "non-nuclear capabilities [to] reduce the role of nuclear weapons in deterring non-nuclear attacks."[105] The United States has participated in various dismantling and downsizing of its nuclear arsenal through many treaties since the end of the Cold War. The United States maintains an unwavering position in maintaining a nuclear weapons arsenal as long as nuclear weapons exist. The U.S. has the largest nuclear energy program in the world, combining private sector production of nuclear energy with government oversight and regulation.[106]

Russian Federation

Like the United States, the Russian Federation has reduced the size of its nuclear arsenal, in addition to increasing transparency about their nuclear stockpile size and capabilities. The Russian Federation's tumultuous, often tense relationship with the United States has resulted in its desire to continue modernization of its nuclear program.[107]

China

China is among those states with nuclear arms capacities. It is worth noting that China has several nuclear weapons systems in the advanced development stage including a new cruise missile, which presumably can carry a nuclear warhead, and new land-launched and sea-launched ballistic missiles. Road mobile nuclear capable missiles add a degree of survivability to China's limited nuclear arsenal. The desire to develop an operational ballistic missile submarine is another suggestion that China is concerned about the survivability of its nuclear forces and perhaps is a comment on its future goals of power projection outside of the immediate Pacific area."[108] China, Russia, and the United States reflect the policy of nuclear-weapons states in that these states are concerned with military escalation, and Great Power conflict. Nuclear weapons provide a level of deterrence that current nuclear-weapons states do not seem positioned to currently relinquish.

European Union

Outside of the United Kingdom and France, the rest of the European Union is a nuclear-weapons free territory, with E.U. members promoting nonproliferation both regionally and globally. Nuclear energy is responsible for 30% of total energy production in the E.U. There are 130 nuclear reactors in operation in 14 EU countries. Each EU country decides alone whether to include nuclear power in its energy supply.[109] The European Union's energy oversight is led by the European Commission. The European Commission remains committed to nuclear safety, radiation protection, safeguarding, waste management, and the decommissioning of nuclear facilities that have reached the end of their usable life cycle.

Latin America

In Latin America, the Treaty of Tlatelolco (Treaty for the Prohibition of Nuclear Weapons in Latin America) requires that no Latin American parties acquire or possess nuclear weapons. In November of 1963, the leaders of Mexico, Brazil, Chile, Ecuador, and Bolivia officially drafted and presented the Treaty to the United Nations General Assembly. Since its implementation in 1967, Latin America's commitment to nonproliferation, like the European Union's, reflects a regional effort for cooperation to avoid nuclear weapons acquisition in Latin American countries.[110]

Africa

The African Nuclear Weapon Free Zone Treaty (Treaty of Pelindaba) marks Africa's efforts and successes at regional cooperation for nuclear nonproliferation. With Burundi serving as the 28th state to ratify as the regional treaty in July of 2009, Africa has officially become a nuclear-weapons free region. Important to note regarding this African treaty is that it "supports the use of nuclear science and technology for peaceful purposes, and in this respect, each Party undertakes to conduct all activities for the peaceful use of nuclear energy under strict non-proliferation measures. The renewed global interest in the development of nuclear power for both electricity generation and for radioactive materials used in medicine, means that the entry-into-force of the Treaty of Pelindaba will have a direct impact on the future nuclear energy developments in African countries."[111]

Questions a Resolution Must Answer

- How can the international community prevent states from developing or acquiring nuclear weapons?
- What can be learned from situation regarding Iran's nuclear program and how can those lessons be applied elsewhere?
- What role does the state play in preventing terrorist groups and other non-state actors from developing or acquiring nuclear weapons?
- What steps can be taken to encourage nuclear disarmament? What incentives do states like the United States and Russian Federation have to disarm their nuclear arsenals?
- How can states cooperate to encourage the spread of nuclear technology for peaceful uses like harnessing nuclear energy?
- How can the international community increase monitoring and regulation standards without infringing on a state's national sovereignty?
- Should the United Nations pursue the establishment of nuclear-weapon-free zones in other areas of the world? In the Middle East?
- How can the international community respond to states that refuse to cooperate with international standards and protocols?
- What methods of radioactive waste management can be implemented in states pursuing nuclear programs? How can these methods be regulated?
- How can the UN, IAEA, and other international bodies help to promote nuclear nonproliferation globally? How can NPT non-

signatory countries be worked with to promote compliance with nuclear nonproliferation?

- Long term creation of sites – how are these site locations determined? How can we implement cost-effective programs that store waste in geologic repositories?
- How can we dispose of waste from security and defense applications?
- How can plans for efficiency standards, regulation, and storage be drafted and implemented? How can oversight be managed?

Conclusion

The challenges that the international community faces regarding the future of nuclear policy will similarly challenge the delegates of this committee. The daunting task before this committee remains finding a way to balance the inevitable rise in nuclear power with the necessary safeguards to deter the spread of nuclear weapons. Such a balance will undoubtedly involve some combination of nuclear disarmament and nuclear non-proliferation. Delegates should be ready to brainstorm innovative ways to encourage implementation and regulation of such safeguards across the global community.

We look forward to an informative and intense debate regarding one of the world's most contentious issues in the 21st century. In your preparation and research, please utilize the many available sources of information regarding this issue. Delegates should come prepared to discuss the many threads of the issue at hand. The collaboration that takes place this weekend will help to broaden our minds and perspectives regarding a complex issue sure to be on the forefront of international policy debate in the 21st century.

Bibliography

[1]"Chapter IV | United Nations." UN News Center. UN, n.d. Web. 22 Apr. 2016. <http://www.un.org/en/sections/un-charter/chapter-iv/index.html>.

[2]"Renaissance -- Printing and Thinking." Renaissance -- Printing and Thinking. N.p., n.d. Web. 17 June 2016.

[3] "Number of Internet Users 2005-2015 | Statistic." Statista. N.p., n.d. Web. 25 June 2016.

[4] Melzer, Nils. Cyberwarfare and International Law. Rep. N.p.: UNIDIR, 2011. Print.

[5] Geers, Kenneth. Strategic Cyber Security. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2011. Print.

[6] "CHM Revolution." ENIAC. Computer History Museum, n.d. Web. 31 July 2016.

[7] "Invention of the Internet." History.com. History, n.d. Web. 26 June 2016.

[8] Ibid.

[9] Ibid.

[10] "The History of Cyber Attacks - a Timeline." NATO. NATO Review Magazine, n.d. Web. 26 June 2016.

[11] Ibid.

[12] Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." Wired.com. Conde Nast Digital, 03 Nov. 2014. Web. 31 July 2016.

[13] Geers, Kenneth. Strategic Cyber Security. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2011. Print.

[14] Ibid.

[15] Ibid.

[16] Krekel, Bryan. Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation. Issue brief. Northrop Grumman Corporation, n.d. Web. 26 June 2016.

[17] Geers, Kenneth. Strategic Cyber Security. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2011. Print.

[18] Maurer, Tim, "Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?", Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.

[19] General Assembly resolution 53/70, Developments in the field of information and telecommunications in the context of international security, A/RES/53/70 (4 January 1999).

[20] General Assembly resolution 55/63, Combating the criminal misuse of information technologies, A/RES/55/63 (22 January 2001).

[21] Maurer, Tim, "Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?", Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.

[22] Vignard, Kerstin. "Perspectives on Cyber War: Legal Frameworks and Transparency and

Confidence-Building." UNIDIR : Research Project. UNIDIR, Feb. 2012. Web. 31 July 2016.

[23] Maurer, Tim, "Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?", Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.

[24] Ibid.

[25] "Counter-Terrorism Implementation Task Force | CTITF." UN News Center. UN, n.d. Web. 31 July 2016.

[26] "The Counter-Terrorism Implementation Task Force (CTITF) | VICTIMS of TERRORISM SUPPORT PORTAL." UN News Center. UN, n.d. Web. 31 July 2016.

[27] Melzer, Nils. Cyberwarfare and International Law. Rep. N.p.: UNIDIR, 2011. Print.

[28] Ibid.

[29] Ibid.

[30] Ibid.

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] Streltsov, A. A. International Information Security: Description and Legal Aspects. Rep. no. UNIDIR/DF/2007/3. N.p.: UNIDR, n.d. Print.

[38] Ibid.

[39] General Assembly resolution 61/54, Developments in the field of information and telecommunications in the context of international security, A/RES/61/54 (20 October 2006).

[40] Maurer, Tim, "Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?", Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.

[41] Ibid.

[42] General Assembly Report of the Group of Governmental Experts 65/201, Group of Governmental Experts on Developments in the field of information and telecommunications in the context of international security, A/65/201 (30 January 2010).

[43] Ibid.

[44] Maurer, Tim, "Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?", Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.

[45] Ibid.

[46] Carr, Jeffrey, and Lewis Shepherd. Inside Cyber Warfare. Sebastopol, CA: O'Reilly Media, 2010. Safari Books Online. Web.

[47] Ibid.

[48] "United Nations Audiovisual Library of International Law." United Nations Audiovisual Library of International Law. N.p., n.d. Web. 31

July 2016.

[49] Fritz, Jason (2008) "How China will use cyber warfare to leapfrog in military competitiveness," Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies: Vol. 8: Iss. 1, Article 2.

[50] Ibid.

[51] "Iran's Military Is Preparing for Cyber Warfare - Flash//CRITIC Cyber Threat News." Flash// CRITIC Cyber Threat News. N.p., 15 Sept. 2013. Web. 17 July 2016.

[52] Zetter, Kim. "We're at Cyberwar: A Global Guide to Nation-State Digital Attacks." Wired.com. Conde Nast Digital, 1 Sept. 2015. Web. 17 July 2016.

[53] "Cybercom Chief Details U.S. Cyber Threats, Trends." U.S. DEPARTMENT OF DEFENSE. N.p., 21 Nov. 2014. Web. 31 July 2016.

[54] "Germany Reveals Offensive Cyberwarfare Capability." Atlantic Council. N.p., 8 Jan. 2012. Web. 17 July 2016.

[55] Cirlig, Carmen-Cristina. "Cyber Defence in the EU Preparing for Cyber Warfare?" EPRS 542.143 (2014): n. pag. European Parliamentary Research Service. EPRS, 01 Oct. 2014. Web. 16 July 2016.

[56] "Turkey: Internet Freedom, Rights in Sharp Decline." Human Rights Watch. N.p., 02 Sept. 2014. Web. 17 July 2016.

[57] Oladipo, Tomi. "Cyber-crime Is Africa's 'next Big Threat', Experts Warn." BBC News. BBC News, 17 Nov. 2015. Web. 17 July 2016.

[58] Ibid.

[59] Melzer, Nils. Cyberwarfare and International Law. Rep. N.p.: UNIDIR, 2011. Print.

[60] Younger, Stephen M. "Nuclear Weapons in the Twenty-First Century." Federation of American Scientists. 27 June 2000. Web. 14 June 2016. http://fas.org/nuke/guide/usa/doctrine/doe/younger.htm.

[61] Ibid.

[62] "Nuclear Power in the 21st Century." International Atomic Energy Agency. 17 June 2013. Web. 14 June 2016. https://www.iaea.org/newscenter/news/nuclear-power-21st-century.

[63] http://energy.gov/ne/nuclear-reactor-technologies.

[64] "History of Nuclear Energy." World Nuclear Association. March 2014. Web. 16 June 2016. http://www.world-nuclear.org/information-library/current-and-future-generation/outline-history-of-nuclear-energy.aspx.

[65] Ibid.

[66] Ibid.

[67] Ibid.

[68] Ibid.

[69] Ibid.

[70] http://www.atomicarchive.com/Fission/Images/fission.jpg.

[71] "Manhattan Project- United States History." Encyclopedia Britannica. Web. 12 June 2016. http://www.britannica.com/event/Manhattan-Project

[72] Ibid.

[73] Ibid.

[74] http://www.atomcentral.com/hiroshima-nagasaki.

aspx

[75] "History of Nuclear Energy."

[76] Ibid.

[77] Adams, Rod. "January 1961: SL-1 Explosion Aftermath." Atomic Insights. 1 July 1996. Web. 27 June 2016. http://atomicinsights.com/january-sl-explosion-aftermath/.

[78] "Backgrounder on the Three Mile Island Accident." United States Nuclear Regulatory Commission. N.p., 12 Dec. 2014. Web. <http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html>.

[79] "Chernobyl Accident 1986." World Nuclear Association. June 2016. Web. 10 July 2016. http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/chernobyl-accident.aspx.

[80] "Fukushima Accident. World Nuclear Association. June 2016. Web. 10 July 2016. http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/fukushima-accident.aspx.

[81] "History of Nuclear Energy."

[82] "Our Work." International Atomic Energy Agency. 21 June 2016. Web. 22 June 2016. https://www.iaea.org/ourwork.

[83] "IAEA Mission Statement." International Atomic Energy Agency. Web. 15 June 2016. https://www.iaea.org/about/mission.

[84] Ibid.

[85] Ibid.

[86] "Member States." International Atomic Energy Agency. 26 February 2016. Web. 15 June 2016. https://www.iaea.org/about/memberstates.

[87] <https://www.iaea.org/about/business>.

[88] "About Us." United Nations Office for Disarmament Affairs. Web. 28 June 2016. https://www.un.org/disarmament/about/.

[89] Ibid.

[90] "Nuclear Power in the 21st Century." International Atomic Energy Agency. 17 June 2013. Web. 29 June 2016. https://www.iaea.org/newscenter/news/nuclear-power-21st-century.

[91] "Nuclear Weapons." United Nations Office for Disarmament Affairs. Web. 22 June 2016. https://www.un.org/disarmament/wmd/nuclear/.

[92] "Treaty on the Non-Proliferation of Nuclear Weapons." Audiovisual Library of International Law.. 2016. Web. 2 July 2016. http://legal.un.org/avl/ha/tnpt/tnpt.html.

[93] http://www.worldtvnews.co.in/?p=47660.

[94] "Nuclear Weapons."

[95] Collina, Tom Z. and Daryl Kimball. "U.S.-Russian Nuclear Arms Control Agreements at a Glance." Arms Control Association. 1 April 2014. Web. 20 June 2016. https://www.armscontrol.org/print/2556.

[96] "Nuclear Weapons."

[97] "1540 Committee - Security Council Committee established pursuant to resolution 1540 (2004)." United Nations. Web. 18 June 2016. http://www.un.org/en/sc/1540/ .

[98] "Nuclear Techniques for Development and Environmental Protection." International Atomic Energy Agency. Web. 28 June 2016. http://www-naweb.iaea.org/na/about-na/index.

html.

[99] "Nuclear Sciences and Applications." International Atomic Energy Agency. Web. 29 June 2016. http://www-naweb.iaea.org/na/about-na/na-our-work.html.

[100] "Global Nuclear Safety and Security Framework." International Atomic Energy Agency. Web. 29 June 2016. http://www-ns.iaea.org/coordination/gnssn.asp?s=110&l=126.

[101] "Disarmament Forum - Nuclear-weapon-free zones." United Nations Institute for Disarmament Research. 2011. Web. 19 June 2016. http://www.unidir.org/files/publications/pdfs/nuclear-weapon-free-zones-en-314.pdf

[102] Ibid.

[103] "Nuclear Arsenals." International Campaign to Abolish Nuclear Weapons. Web. June 29 2016. http://www.icanw.org/the-facts/nuclear-arsenals/.

[104] "Nuclear-Weapon-Free Zones." United Nations Office for Disarmament Affairs. Web. 21 June 2016. https://www.un.org/disarmament/wmd/nuclear/nwfz/

[105] "Nuclear Weapons Employment Strategy of the United States." The White House - Office of the Press Secretary. 19 June 2013. Web. Accessed 27 June 2016. https://www.whitehouse.gov/the-press-office/2013/06/19/fact-sheet-nuclear-weapons-employment-strategy-united-states.

[106] "US Nuclear Energy Policy." World Nuclear Organization. Web. Accessed 26 June 2016. http://www.world-nuclear.org/information-library/country-profiles/countries-t-z/usa-nuclear-power-policy.aspx.

[107] "Russia." Nuclear Threat Initiative. March 2015. Web. Accessed 28 June 2016. http://www.nti.org/learn/countries/russia/.

[108] Ibid.

[109] "Nuclear Energy. European Commission. 1 January 2016. Web. Accessed 25 June 2016. http://ec.europa.eu/energy/en/topics/nuclear-energy.

[110] "Latin America Nuclear Weapons Free Zone Treaty (Treaty of Tlatelolco)." Arms Control Association. Web. Accessed 22 June 2016. https://www.armscontrol.org/documents/tlatelolco.

[111] "Africa is Now Officially a Zone Free of Nuclear Weapons." Institute for Security Studies. 12 August 2009. Web. Accessed 29 June 2016. https://www.issafrica.org/iss-today/africa-is-now-officially-a-zone-free-of-nuclear-weapons.