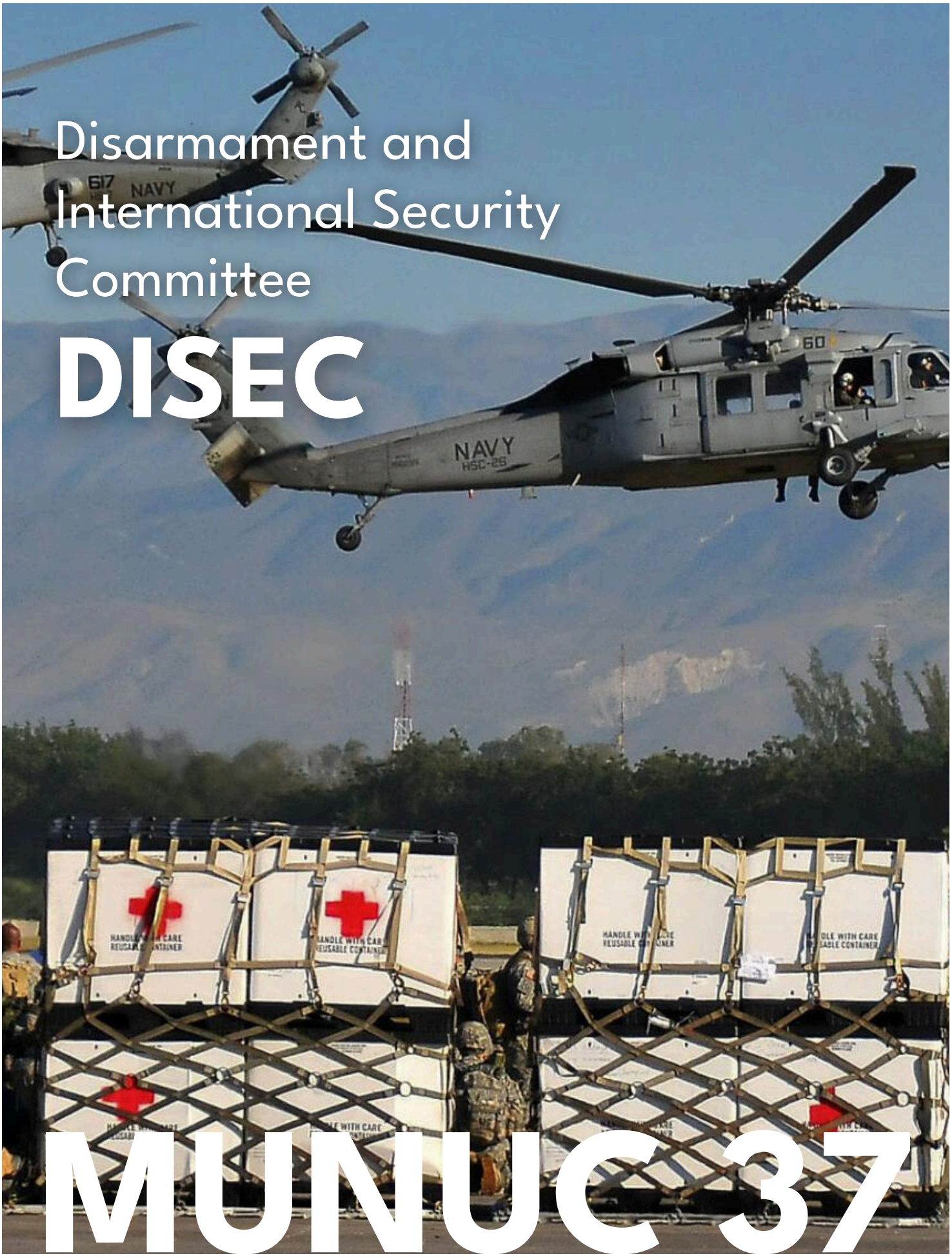


Disarmament and International Security Committee

DISEC

MUNUC 37

Model United Nations of the University of Chicago

Chair Letter

Hello Delegates,

Welcome to MUNUC 37 and the First Committee of the General Assembly, the Disarmament and International Security Committee (DISEC)! I am very excited to be one of your chairs this year, and I am greatly looking forward to a weekend of fantastic debate and substantive solutions.

I am Anna Falcone, one of the three chairs in this committee alongside Alex and Hari. I am a fourth year in college, majoring in Religious Studies and Law, Letters, and Society. I grew up in New York City. In terms of Model UN, I am a chair for ChoMUN, our collegiate Model UN conference, and I am one of the presidents of the University's Travel Model UN team. Over the past two years, I have chaired SOCHUM at MUNUC 36 and DISEC at MUNUC 35. I have also chaired WTO at WeMUN Expo in Beijing. I usually compete in General Assembly committees, so they are my favorite kind of committees. Beyond Model UN, I am somewhat involved in the Institute of Politics, and I tend to watch a lot of TV and hang out with friends in my free time.

I am so excited to be chairing a General Assembly again and to be chairing this committee. Hari, Alex and I really want to facilitate both a fun and respectful committee environment. We really want to see delegates work together and speak their minds in order to find new and creative solutions to the issues surrounding drones and cybersecurity. Personally, I am particularly interested in new creative solutions that address drones both in and out of the context of warfare.

Just a couple of tips from me. First, I value collaboration and respect more than anything else in the committee. This activity is about working together to find the best possible solutions to the issues at hand. I will not look favorably upon people who talk over other delegates, delete their work, or exclude them in order to try and control a bloc. I want to create a space where everyone can share their ideas and have a good time overall in

committee. Additionally, I am really looking for interesting and creative solutions to the problems addressed in committee. Try to think out of the box and beyond what is already being done in order to find new and more effective solutions. Lastly, this is a really big General Assembly committee and I know that can be intimidating (trust me I have been there), and I really commend you all for taking this on. I really hope you all participate in both front room and back room, as I am sure you all have excellent ideas to share.

If you have any questions on the topic, committee procedure, Model UN at large, or anything else please feel free to email me at afalcone@uchicago.edu. See you in February!

Best,

Anna Falcone

Dear Delegates,

Welcome to MUNUC 37! I am Hari, and I will be one of your chairs for the First Committee of the General Assembly, the Disarmament and International Security Committee (DISEC). I am super excited to be your chair and I look forward to a great weekend of debate and collaboration!

Just so you know a little about myself, I am a 4th year student at the University of Chicago majoring in Mathematics and Economics. I grew up in San Jose, California for most of my life before moving to the beautiful city of Chicago. I spend my time on campus participating in on campus research as a student research assistant and writing my senior thesis. In terms of Model UN, I plan to chair a committee at UChicago's collegiate conference, ChoMUN, and compete with the travel team. Last year, I was the USG of Specialized Agencies for MUNUC, and the year prior I was the EAC for a crisis committee.

I am super excited to chair a large General Assembly–specifically the DISEC. We expect great ideas, interesting debate, and enthusiastic participation from all of you. Most importantly, your enthusiastic participation needs to uphold our most important principles of collaboration and diplomacy, which involves listening to your peers and advocating for your own ideas while respecting others and their ideas (remember the Golden Rule!). This means you shouldn't talk over delegates, dismiss others' ideas, or create an environment in the bloc where other delegates don't feel like participating. This weekend is going to be an exciting time for all of you to discuss new, creative, and positive solutions to our topics of discussion. You as delegates will get the most out of this opportunity if you remember the importance of collaboration and diplomacy.

On to my thoughts on the topics and solutions, you may notice that my co-chair Anna is particularly interested in hearing debate on the topic of drones, but personally I find cybersecurity to be an extremely important issue to address in a modern, rapidly changing world. Regardless of which topic gets picked for debate, I expect your solutions to be creative in addition to being substantive. The background guide will go over prior

solutions to these issues as a way to guide your planning, but you should think of your own unique solutions to propose during debate.

Lastly, I want you all to congratulate yourselves for taking this step and participating in a large GA. You will notice on the first day of the committee that there are hundreds of other delegates in this room who have spent the past few months preparing–just as you will have–for this committee. Take this opportunity to participate in the backroom by writing clauses, stand up in the frontroom to give a speech, and attend the workshops put on by MUNUC to improve your experience in committee. If you have any questions, shoot me an email at harikesanb@uchicago.edu.

Best,

Hari Balachandran

History of the Committee

The Disarmament and International Security Committee (DISEC) is the First Committee of the United Nations General Assembly. This committee is tasked with writing resolutions that consider all issues regarding "disarmament, global challenges and threats to peace" as described in the UN Charter.[1] The committee works in tandem with the United Nations Disarmament Commission and the Geneva-based Conference on Disarmament.[2] As DISEC is a part of the UN General Assembly (UNGA), each of the 193 Member States are allowed to participate and each member state has an equal vote on every matter.[3]

In the 78th session of the General Assembly, which took place in September 2023,[4] DISEC looked at issues that ranged from reducing military budgets to preventing an arms race in outer space to many issues concerning nuclear disarmament around the world.[5] While the resolutions passed are not binding, as in every other General Assembly committee, these documents can play a huge part in guiding international conversation and helping with coordinated global efforts.[6]

---

[1] "Disarmament and International Security (First Committee)," United Nations, accessed August 11, 2024, https://www.un.org/en/ga/first/.

[2] Ibid.

[3] "Workings of the General Assembly," United Nations, accessed August 11, 2024, https://www.un.org/en/ga/.

[4] "High-Level Meetings of the 78th Session," United Nations, accessed August 11, 2024, https://www.un.org/en/ga/78/meetings/.

[5] "Allocation of Agenda Items to the First Committee," United Nations General Assembly, accessed August 11, 2024, https://documents.un.org/doc/undoc/gen/n23/320/16/pdf/n2332016.pdf.

[6] "How Decisions Are Made at the UN," United Nations, accessed August 11, 2024, https://www.un.org/en/model-united-nations/how-decisions-are-made-un#:~:text=Given%20the%20dramatic%20increase%20in,possible%20implementation%20of%20GA%20decisions.

Topic A: Drones

Statement of the Problem

The development and implementation of drones can provide many benefits. It can allow companies to inspect infrastructure easily and safely, and it can allow NGOs to bring humanitarian aid into hard-to-reach places or allow emergency response agencies to quickly evaluate situations. However, with all of this power there comes many risks. Drones can also allow law enforcement or even private citizens to record and collect information on people without their knowledge. Drones can also quite simply be dangerous as they can crash into things. Military drones can be involved in strikes that might kill unintended targets.

Military and Law Enforcement Drones

Military drones are able to be used from distant locations to kill individuals or destroy infrastructure. Ever since the first drone strike, authorized by U.S. President George W. Bush in 2002, drones have become commonplace in the arsenal of both military and stateless actors. Drone warfare brings up all sorts of concerns regarding what a legitimate usage of drone strikes are. The ethics of drone strikes often comes down to considerations about civilian protection, the advancement of security, and the risk to soldiers in the area. These three factors in particular can be used to determine whether drone strikes can be ethical or legitimate in the public eye and in warfare.[7] When considering military drones, it is important to consider how drones can be used critically and without causing unnecessary damage and harm, if they are used at all.

[7] Paul Lushenko, "The Moral Legitimacy of Drone Strikes: How the Public Forms Its Judgments," Texas National Security Review, March 3, 2023, https://tnsr.org/2022/11/the-moral-legitimacy-of-drone-strikes-how-the-public-forms-its-judgments/.

A U.S. Marine launching a drone in Mykolaivka, Ukraine in 2017.[8]

Drones are also used in law enforcement contexts. These include circumstances where there are hostages taken or active shooters. These drones are able to give law enforcement tactical teams real-time information. The surveillance capability of drones allows law enforcement to monitor crowds at events or protests.[9] However, law enforcement's surveillance usage of drones has come under some heat. In New York, there was a huge debate weighing drone usage versus privacy concerns. There is a battle between utilizing drones to react to a natural disaster or an emergency of a similar size, while not overusing drones to monitor crowds or protests where people

[8] "Mykolayivka, Ukraine (July 19, 2017) a U.S. Marine with Black Sea Rotational Force 17.1 Launches an Unmanned Aerial Vehicle during Exercise Sea Breeze 2017 in Mykolayivka," rawpixel, accessed September 1, 2024, https://www.rawpixel.com/image/3393500/free-photo-image-drone-aerial-vehicle-armored.

[9] "Top 10 Commercial Uses For Drones | Inspired Flight Technologies," accessed August 29, 2024, https://www.inspiredflight.com/news/top-10-commercial-uses-for-drones.php.

might feel that their First Amendment rights are violated.[10] While not every country's citizens have freedoms similar to those included in the U.S. Constitution's First Amendment, the conflict between privacy and security needs to be considered when it comes to drone usage in law enforcement contexts.

Humanitarian Drones

Drones are incredibly helpful in both humanitarian and development situations. Oftentimes, United Nations organizations will utilize drones to carry out key functions. One example of this is UNICEF. UNICEF and its partners are looking into drone technology to aid in projects like vaccine delivery and transportation, accessing hard-to-reach communities, and emergency preparedness and response with aerial imaging. Drones are critical in this kind of work because they combine fast speeds and built in monitoring systems that can make transportation of critical supplies more efficient and effective.[11] For example, if someone needs a vaccine transported at a certain temperature at a certain time, a drone could get the vaccine to the location quickly while monitoring the temperature to make sure the vaccine is still effective. UNICEF also believes that drones can be especially helpful and critical in medical emergencies when diagnostic kits or medical supplies are needed.[12]

The World Food Programme (WFP) is also a big proponent of drone usage as it can aid in critical cargo delivery. While the WFP does not think that drones can replace other humanitarian vehicles like 4x4s or planes, they do have the added benefits of not needing infrastructure like roads or runways to operate.[13] The WFP writes "[d]rones are playing a progressive and influential role in humanitarian emergency preparedness and response...

---

[10] ABC7 New York, "Invasion of Privacy? Debate Wages over Drone Use by Police in New York," August 22, 2023, https://abc7ny.com/new-york-drones-invasion-of-privacy-police-departments/13685989/.

[11] "Drones," UNICEF, n.d., https://www.unicef.org/innovation/drones.

[12] Ibid.

[13] "Using Drones to Deliver Critical Humanitarian Aid | WFP Drones," accessed August 29, 2024, https://drones.wfp.org/updates/using-drones-deliver-critical-humanitarian-aid.

with their ability to heighten efficiency and precision, drones can raise humanitarian response to new levels and deliver benefits to affected communities."[14]

Other than delivering aid, drones can also be used to conduct search and rescue initiatives. Drones are able to quickly look around areas and utilize advanced imaging technology to look for heat signatures and signs of human presence. Drones' ability to do this quickly can help save even more people in case of emergency.[15] One example of drones' ability to utilize imaging is when they combat fires. In firefighting situations, drones are able to image and communicate information about burn spots in forests and fire intensity, allowing firefighters to stay safe and remain informed.[16]

Humanitarian drone usage lends itself to a very specific set of ethical concerns. The first being concerns weighing the harm versus benefit of drone usage. When using humanitarian drones in particular, it is critical to set up frameworks that will ensure that harm is minimized. These frameworks can take the form of simply making sure that a drone does not crash and accidentally hurt a person, or can be slightly more complicated by considering the environmental impacts of drone usage or minimizing data collection to ensure privacy considerations are met. At the same time as considering how to minimize the harm of drone usage, it is critical to maximize the benefit of drones. The specific benefits of drones should be evaluated, which can be done by answering questions such as "does the drone actually deliver the goods it needs to?", as well as considering the general goal of drone usage, such as ensuring a drone delivering vaccines helps the broader healthcare crisis.

---

[14] "WFP Drones," June 25, 2024, https://drones.wfp.org/.

[15] "Top 10 Commercial Uses For Drones | Inspired Flight Technologies," accessed August 29, 2024, https://www.inspiredflight.com/news/top-10-commercial-uses-for-drones.php.

[16] Drones For Good Worldwide, "DronesForGood - Worldwide | Donate Today To Save Lives," accessed August 29, 2024. https://dronesforgoodworldwide.org/; "Drones for Firefighting," accessed August 29, 2024, https://www.skydio.com/solutions/public-safety/fire-fighting-drones/.

Humanitarian drones also carry with them a set of questions regarding cost. It is important to consider who is paying for humanitarian drones and how that can impact their usage. Should countries be individually paying to provide humanitarian drone coverage? Should NGOs be mainly funding those efforts? Additionally, there should also be liability concerns. If a country pays to send a drone with aid to another area and the drone crashes, who is liable for any damage done?

The last consideration with humanitarian drones regards privacy and consent. It is important to make sure that communities receiving drone aid actually want the aid, and that privacy is respected for individuals receiving aid. Drones have the unique ability to cross boundaries and collect information in ways not seen before, but it is important to consider how those traits can be used but not abused.[17]

Commercial and Recreational Drones

Drones are not always used for official government purposes. Drones also have private sector usages separate from warfare and humanitarian purposes. People can buy drones and utilize them for recreational and commercial purposes, such as taking photos or videos, delivering packages, or just flying them around for fun. The biggest complication in the drone industry is that the laws that regulate different private sector usages vary from one country to the next. Some countries allow their citizens to use drones relatively freely, others require paperwork for drone usage, and a third set forbid the usage of drones altogether. These differences mean that consumers need to be aware of the regulations regarding drones in the place that they reside in.[18]

---

[17] Ning Wang, Markus Christen, and Matthew Hunt, "Ethical Considerations Associated with 'Humanitarian Drones': A Scoping Literature Review," Science and engineering ethics, August 3, 2021, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8330183/.

[18] Dronemade, "Dronemade | Country Drone Laws 2024 | World Map," accessed August 29, 2024, https://www.drone-made.com/drone-laws.

While many commercial drones are still sold to the military, government, or law enforcement, corporations might also buy drones for purposes such as being used for inspections and surveillance in a variety of sectors. One of these applications is in infrastructure inspections, as drones have the ability to get to hard-to-reach locations in a safer and cheaper manner. These drones are able to look at different buildings and bridges both to inspect for structural issues and to monitor the progress of a construction project. Drones can also play this role in the energy industry as they inspect solar panels, wind turbines, and power lines looking for any damage or issues. One example of this is drones with thermal cameras, which can monitor power lines and solar panels for hotspots that could give rise to electrical issues. Drones also have applications in agriculture and precision farming, aerial photography, mapping and land surveying, and environmental monitoring.[19]

Recreational drones are used for different purposes all together. According to the US government, recreational drone usage is "is flying for enjoyment and not for work, business purposes, or for compensation or hire."[20] Sometimes people will just fly drones because they think it's fun, or maybe to capture a unique video from high up. These purposes don't bring the individual any monetary gain, but instead are just for pure enjoyment.

There are a few potential issues when it comes to recreational drone usage. The first issue is privacy concerns. When people are able to fly around cameras with little to no regulation, it can put other people's privacy at risk. The question over privacy and drone flight can add to current conversations around concerns of "public" privacy and "private" privacy–that is, concerns about what actions should be protected under privacy rights.[21]

---

[19] "Top 10 Commercial Uses For Drones | Inspired Flight Technologies," accessed August 29, 2024, https://www.inspiredflight.com/news/top-10-commercial-uses-for-drones.php.

[20] "What Is the Definition of Recreational or Hobby Use of a UAS or Drone?," Federal Aviation Administration, accessed September 1, 2024, https://www.faa.gov/faq/what-definition-recreational-or-hobby-use-uas-or-drone#:~:text=Recreational%20or%20hobby%20UAS%20or%20drone%20use,the%20ordinary%2C%20dictionary%20definition%20of%20these%20terms.

[21] Wells C. Bennett, "Civilian Drones, Privacy, and the Federal-State Balance," Brookings, March 9, 2022, https://www.brookings.edu/articles/civilian-drones-privacy-and-the-federal-state-balance/.

Another potential issue with private drone usage is concerns over drones crashing and causing damage. Drones have crashed into commercial planes, people's windows, US Army Black Hawks, and even the Empire State Building. There was once even a drone that landed on the White House lawn. Drone usage around planes can cause real safety and security issues as they could distract pilots or damage the plane, ultimately causing crashes and loss of life.[22]

Overall, the two major considerations when it comes to both humanitarian, commercial, and recreational drone usage are safety and privacy. It is important to consider how international frameworks can ensure that drones do not cause unnecessary damage or harm, while still maximizing any potential benefit they could bring. An example of this is looking at how a drone can deliver medical supplies without potentially crashing into a helicopter trying to do the same thing. Additionally, with recording capabilities being added to drones, how can international bodies ensure that privacy is protected? Does it make sense to limit data storage or data collection? Is there a way to protect people from having their lives recorded by other private citizens or governments, and how can international bodies aid in that?

[22] "First Drone Crash with a Commercial Aircraft in Canada Triggers Safety Review and Possible New Rules," EDI Weekly: Engineered Design Insider, June 21, 2017, https://www.ediweekly.com/first-drone-crash-commercial-aircraft-canada-triggers-safety-review-possible-new-rules/.

History of the Problem

Early Drones

In 1907, the quadcopter was invented, which was the first innovation that brought the world closer to drones occurred.[23] A quadcopter is made up of four propellers stabilized at a central point, as seen in the photo below. This initial invention was created by brothers Jacques and Louis Breguet and Nobel Prize winner Professor Charles Richet. While the initial quadcopter could not get more than two feet off the ground and needed four men to steady it, it did lead to the current quadcopter form that is used today!

The structure of a basic quadcopter.[24]

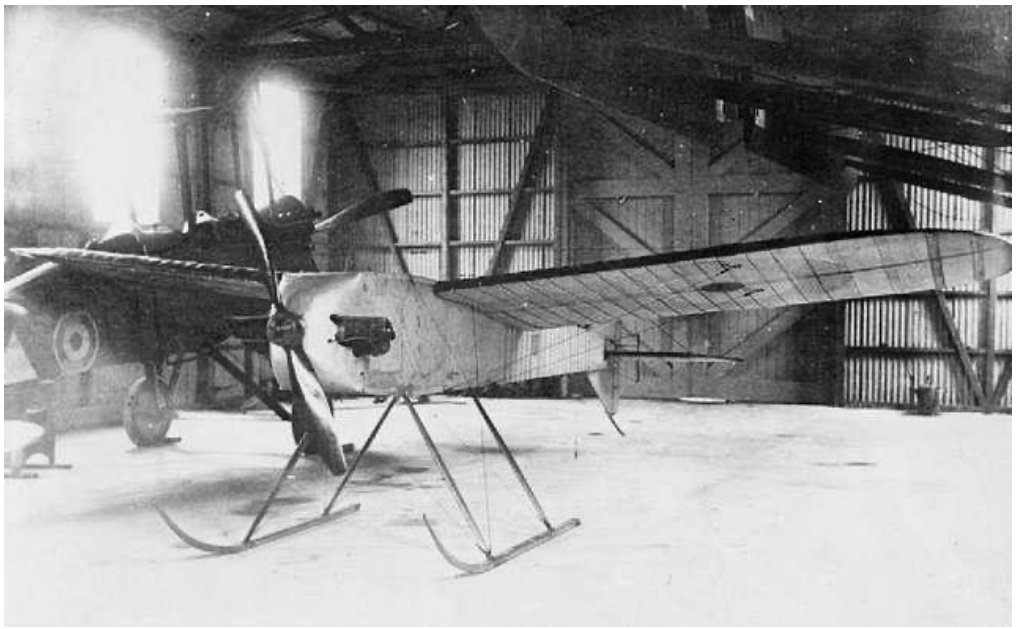
The first military drones took another ten years to be invented. In 1917, during World War I, the Ruston Proctor Aerial Target was launched, which was the first pilotless winged aircraft. This aircraft was essentially a

---

[23] Digital Trends, "The History of Drones in 10 Milestones," September 11, 2018, https://www.digitaltrends.com/cool-tech/history-of-drones/.

[24] Ali.yusuf7, *"A Quadcopter Based on the Plus Design Configuration, with a Light Weight Aluminum Frame and Powerful 1000 Kva Motors,"* December 3, 2014, https://commons.wikimedia.org/wiki/File:Quadcopter_-_Plus_Design.JPG.

radio-controlled pilotless airplane which was based on Nikola Tesla's radio-control technology. These drones were meant to essentially just act as bombs and therefore were only meant to be used by the military. The plan was to steer them from a remote location into enemy encampments. Despite the invention of such a novel technology, this drone was never actually used and instead was a starting point for the invention of other types of military drones.[25]



The Ruston Proctor Aerial Target aircraft.[26]

Similar drones were being created in the United States. In 1917, Charles F. Kettering invented the Unmanned Kettering Aerial Torpedo, also known as the Kettering Bug. This drone was launched off a portable track and had electrical controls that could stabilize it. At some point, the electrical controls would turn off and

---

[25] "The History of Drones in 10 Milestones."

[26] *"Aircraft and Balloons Used by Some of the Air Pioneers Who Were Contemporary With Samuel Franklin Cody,"* https://commons.wikimedia.org/wiki/File:Ruston,_Proctor_Radio_controlled_target_aircraft_RAE-O870.jpg.

the Bug would fall to the ground, detonating 180 pounds of explosives. Less than 50 of these drones were built before the World War I armistice was signed, and none of them were used.[27]

It was not until 1934 that a remote-controlled weapon was actually put to use. The German military invented the FX-1400, or the "Fritz X", during World War II. This weapon was a 2300-pound bomb primarily used for sinking ships. This drone was successfully deployed and paved the way for other similar remote-controlled missiles.[28]

In the 1960s, there was advancement in transistor technology that changed the course of how drones were developed and utilized. During this decade, miniaturized radio-controlled components became accessible to consumers. This led to a huge increase in the number of radio-controlled planes sold in the US. These planes came in a variety of models that could be used inside or outside. The innovations in transistor technology that made this possible created a consumer market for drones. Drones were no longer just a weapon of war, but also a product people could buy.

Modern Drone-Based Military Operations

In the last twenty years there have been great innovations in drones as technology has continued to advance, but there have also been many instances of drones causing significant damage.

The first drone-based kill operation was conducted by the CIA during the aftermath of 9/11.[29] On February 4, 2002, the American government used a Hellfire missile from a pilotless Predator drone to attack a group of people who they suspected to be Al Qaeda leaders. This attack, however, ended up killing three innocent

---

[27] "Kettering Aerial Torpedo 'Bug'," National Museum of the United States Air Force, n.d., https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/198095/kettering-aerial-torpedo-bug/.

[28] Digital Trends, "The History of Drones in 10 Milestones."

[29] Ibid.

men, named Daraz Khan, Jehangir Khan, and Mir Ahmed, who had traveled to collect scrap metal. The CIA had thought that these men might be powerful members of Al Qaeda, and in particular thought that 5-foot-11 Daraz Khan might be one of Al Qaeda's foremost leaders. This attack caused backlash from the people in the neighboring village.[30] Shawol Khan, Daraz's older brother, was quoted in the New York Times saying "Surely, it was a big mistake of the Americans. They should know that there are no Al Qaeda here. We are very poor people, and we know nothing of politics."[31] This attack presents a couple of major ethical concerns of drone warfare, specifically that strikes from distance may kill a person mistaken for someone else, or that these strikes can kill civilians in addition to hitting the target. Drones are a double-edged sword, as they make it possible for attacks to be carried out without soldiers' lives being put at risk, but at the same time they remove the element of on-the-ground decision making and make the impacts of actions feel more distant, often leading to unnecessary deaths.

Military use of drones has exponentially grown in the last 10 years. Before 2014, only the United States, Israel, the United Kingdom, and China really had drones. As of 2023, around 40 countries are in possession of MALE drones,[32] or Medium Altitude Long Endurance drones.[33] Different countries mostly source them from either China or Turkey, with a smaller subset sourcing drones from internal development, the United States, Iran, and Israel. These drones can be used to both strike within the borders of the country who owns them or in another

---

[30] John F. Burns. "A NATION CHALLENGED: THE MANHUNT; U.S. Leapt Before Looking, Angry Villagers Say," *The New York Times*, February 17, 2002, sec. World., https://www.nytimes.com/2002/02/17/world/a-nation-challenged-the-manhunt-us-leapt-before-looking-angry-villagers-say.html.

[31] Ibid.

[32] Drone Wars UK, "Who Has Armed Drones?," February 4, 2019, https://dronewars.net/who-has-armed-drones/.

[33] "Medium Altitude Long Endurance - an Overview | ScienceDirect Topics," accessed August 29, 2024, https://www.sciencedirect.com/topics/engineering/medium-altitude-long-endurance#:~:text=2.2%20Based%20on%20Altitude%20and%20Range&text=NATO%3A%20UAVs%20with%20an%20altitude,range%20less%20than%20200%20km.

country. While many countries are using these MALE drones, there has also been the more recent proliferation of one-way attack drones that cannot be reused.[34]

Commercial Drone Advancement

The first sign of a possibility of a commercial drone market occurred in 2006. At this time, the US Federal Aviation Administration created commercial drone permits. These permits opened the door for the creation and usage of commercial drones, a market that took off soon after the permits were created.

In 2010, Wi-Fi-controlled drones hit the market from the French company Parrot. These drones allowed even more people to use drones, especially as piloting technology was made more accessible for new users.

In 2013, the idea of drone delivery hit the media, as Jeff Bezos and Amazon put out concept videos for a drone-based delivery system. While Amazon was not the first company to think of this, this concept video did lead to drone deliveries hitting the mainstream media. However, these deliveries have not actually taken place as it would require changes to federal law.[35]

In 2013, DJI, a company founded in 2006, developed and produced the Phantom series drone. This drone was among the first to have a camera, allowing users to take videos and photographs. Soon after this drone was put to market, DJI led the consumer drone market, with over 80% of drones being developed by the company.[36] One thing to consider about commercial drone innovation like this is how to balance the benefits of advancement with potential risks to safety and security. Because of inventions like the Phantom series drone,

---

[34] Drone Wars UK, "Who Has Armed Drones?."

[35] Digital Trends, "The History of Drones in 10 Milestones."

[36] rshaffer. "A Not-So-Short History of Unmanned Aerial Vehicles (UAV)." Consortiq, June 10, 2020. https://consortiq.com/uas-resources/short-history-unmanned-aerial-vehicles-uavs.

private citizens are able to utilize the camera functions and capacity of a drone in the sky, which could infringe on privacy rights in certain countries.

Past Actions

UN Action

In 2021, the UN created the Global Counter-Terrorism Programme on Autonomous and Remotely Operated Systems (AROS), which is meant to help member states respond to threats posed by drones and similar technologies. This program was developed in response to both the quick progress in drone technology and the reality that these technologies can pose real risks to safety and security in the hands of terrorist groups. The program works to achieve a set of objectives through a series of approaches. The program helps to carry out the United Nations Global Counter Terrorism Strategy (A/RES/60/288) and its 8th review focused on drone technologies. Beyond this, the program also supports a host of UN Security Council Resolutions as well as other UN aims and agreements.[37]

[37] "Autonomous and Remotely Operated Systems | Office of Counter-Terrorism," accessed August 29, 2024, https://www.un.org/counterterrorism/autonomous-and-remotely-operated-systems.

A meeting of the UN Security Council, an important body that also aims to promote counterterrorism initiatives including protections against drone attacks.[38]

AROS has three key objectives. The first is to spread and exchange knowledge on "good practices and guidance related to autonomous and/or remotely operated systems". This objective is simply to share information and ensure that the global community is educated on how to best utilize and interact with drone technologies in order to ensure everyone's safety. The second objective is to help member states have the ability "to counter terrorist threats related to AROS". This objective focuses on how the international community can band together to ensure that every member state is protected against drone attacks. The last objective is to promote the use of drone technologies in "non-lethal/non-kinetic human rights-compliant purposes". These three objectives together aim to spread information to help member states guard themselves from attacks, while also promoting drone usage for humanitarian and commercial purposes. These objectives do not look to stop prohibiting

[38] "The Security Council," Flickr, September 2, 2024, https://www.flickr.com/photos/un_photo/24320174321.

innovation, but instead are focused on ensuring that any advancement is done in a manner that follows international humanitarian law and adheres to basic human rights.[39]

This program operates in a handful of key ways. On the education front, the program works to bring together experts and establish partnerships between "Member States, intergovernmental organizations, the private sector, and civil society" to ensure that information can be spread. The program also works to create training courses and training products for anyone involved in the field of drone technology. Additionally, the program publishes research aiming to lead and advance the conversation on drone technology. Lastly, on a more tangible level, the program looks to "provid[e] equipment to support national capabilities to use and/or counter AROS". Together, these different actions ensure that the objectives of the program are pursued efficiently and effectively.[40]

Private and Commercial Drone Usage

One of the main issues in drone usage worldwide is that different countries have different kinds of laws regarding drones. Some countries have practically banned the usage of drones within the country. Morocco is one of a handful of countries with fairly strict drone regulations, so strict in fact that it is practically a complete ban. In Morocco, drone importation and private use is prohibited, and companies can only use drones with special permits.[41]

Drone laws in Morocco have the largest impact at customs and when it comes to company usage. If someone brings a drone into Morocco without declaring it, the drone will be seized and the person will not be able to get the drone back. If a drone is declared, customs will hold onto the drone, and there is a chance that the person can get it back when leaving the country. There are also a handful of commercial drone regulations. First,

---

[39] Ibid.

[40] Ibid.

[41] Francis Markert, "Drone Rules and Laws in Morocco - Current Information and Experiences," Drone Traveller, February 25, 2018, https://drone-traveller.com/drone-laws-morocco/.

the company desiring to use drones must go through a long and arduous approval process to be granted permission to use a drone. After getting permission, the company must follow a set of rules that are very strictly enforced, which include not flying the drone "over people or large crowds", "over airports or in areas where aircraft are operating", and only flying "during daylight hours and... in good weather conditions". All in all, drone usage in Morocco is highly limited and closely regulated by the Moroccan government.[42]

Compared to Morocco, drone laws in Singapore are similar in some ways but different in others. The biggest difference is that in Singapore, a permit is not required if a person is flying a drone that "weighs 7 kilograms (15 pounds) or less that is being flown 200 feet or below". This means that both private individuals and commercial organizations can easily utilize drones. However, there are similarities between Moroccan and Singaporean drone laws when it comes to when and where drones can be flown. Like Morocco, in Singapore a person cannot fly a drone "over people or crowds", "within 5 kilometers (3.1 miles) of an airport", and can only fly "during daylight hours" and must maintain "a visual line of sight with their drone at all times".[43]

[42] p-themes, "Morocco Drone Laws," UAV Systems International, accessed August 29, 2024, https://uavsystemsinternational.com/pages/morocco-drone-laws.

[43] UAV Coach, "Drone Laws in Singapore | UAV Coach (2023)," accessed August 29, 2024, https://uavcoach.com/drone-laws-singapore/.

An image of a commercial drone flying high above a green landscape.[44]

[44] Miriam McNabb, "All SIM Cards Are Not the Same: The Risks of Using Consumer SIM Cards for Drone Operations," DRONELIFE, January 16, 2023, https://dronelife.com/2023/01/16/all-sim-cards-are-not-the-same-the-risks-of-using-consumer-sim-cards-for-drone-operations/.

Possible Solutions

Building on AROS Objectives

Delegates should consider how they can either continue to fulfill the aims of the AROS program discussed in the "Past Actions" sections or any other UN agreements or if there is a different direction that must be taken to properly regulate drone usage. Delegates should specifically look at issues that this program does not address, especially regarding how member states should regulate commercial drones in order to ensure that they do not cause harm. Utilizing frameworks established by past UN actions and determining their holes can be critical to figuring out how the UN can best move forward when it comes to drone technologies.

To effectively build on these objectives, delegates can consider creating a platform for countries to discuss and create innovative counterterrorism initiatives to defend against attacks from drones. As has been thoroughly discussed, drones are an easy way for both militaries and terrorist organizations to efficiently carry out targeted attacks without risking lives of their own. Furthermore, large-scale drone attacks are often quite effective and have shown to be very difficult to stop. Creating an information-sharing and collaboration platform for countries will ensure that terrorism caused by drones can be reduced and limited significantly.

Improving Data Collection Systems

In addition to building on pre-existing AROS objectives, delegates should consider how to emphasize humanitarian issues in their resolutions, as it is critical to ensure that drones are not causing unnecessary harm, such as killing civilians. Furthermore, it is important to consider how drones can be used specifically to provide humanitarian aid. These considerations can help delegates figure out how the global community can come together to innovate in productive and helpful ways instead of harmful and destructive ones.

The creation of a large-scale database to collect data on drone usage and impact globally could help significantly reduce civilian casualties caused by drones. The database can collect data on military drones,

including how many each country launches and how many casualties they result in and can sort the casualties in categories of "target" and "civilian". If a drone results in a number of "target" casualties and few to none "civilian" casualties, that is a sign that it was effective, but if the opposite is true, this drone should be inspected and an investigation should be conducted to determine what went wrong. If a pattern of high "civilian" casualties caused by drones launched by a specific country is observed, this could serve as grounds for further investigations. Countries can be encouraged to join this database as it aims to cut down on drone-caused civilian harm and ultimately make drones safer and more effective.

Also, as mentioned earlier in the background guide, there are drones that are used specifically for humanitarian purposes, such as transporting needed medical supplies to a hard-to-reach location. It is important that these sorts of drones stay in use, and that data is also collected on these drones to ensure that their efficiency and efficacy can be evaluated and ultimately improved. In fact, in instances where drones unnecessarily cause harm to civilians, these humanitarian drones can be used to quickly provide aid to the region where there are injured civilians to ensure that first responders have the supplies they need to effectively treat them.

Creating Uniform Drone Safety and Privacy Regulations

Given the examples of Moroccan and Singaporean drone laws and the similarities between them, there might be some regulations regarding drone usage that can be made uniform across many countries. These regulations might include standards regarding where drones can be flown to ensure that privacy rights are not violated. They may also include standards that prevent private and commercial drones from interfering with other forms of air travel to ensure that everyone is safe in the global airspace. They might also be more specific regarding the time of day a drone can be flown or the kinds of drones that might need permits to be flown.

Additionally, delegates should look into ways that the international community can come together to resolve differences in drone laws between countries. How should a country with a drone ban interact with a

country that does not require drone permits at all? There are many different perspectives and questions that should be considered as delegates think of comprehensive ways to address drone usage worldwide.

Bloc Positions

One dividing line in this committee is the rules and regulations already put in place by a Member State's government regarding drone usage. These differences might cause member states to have different priorities when it comes to creating and implementing international standards for drones.

Countries With Commercial or Private Drone Bans

Some countries might have drone bans or a near ban on drones, such as Morocco. Additionally, countries that are often negatively impacted by military drone usage might be in favor of more regulation. These countries might prohibit the importation or private usage of drones. A country like this might advocate for these sorts of strict regulations to be more prevalent throughout the rest of the world and may bolster drone bans by pursuing increasingly harsh regulations on the commercial use of drones. Additionally, these countries might be less interested in promoting drone trade as it might go against legislation within the country.

Countries With Few Commercial or Private Drone Regulations

Other countries might not have especially harsh drone laws and instead might allow fairly unfettered use of drones, such as Singapore. Additionally, countries that heavily rely on drone usage in military pursuits might not want international restrictions on governmental drone usage either. These countries might be more interested in having international standards that support and promote the usage of drones. They might look to promote international trade of commercial drones and encourage the innovation of new private and commercial drones. These countries would probably aim for regulations that add more restrictions to drone usage to allow for the usages already permitted within the member state.

Glossary

Drone – A drone is an aircraft that operates via remote control without a pilot physically present in the drone. These machines can perform a range of tasks from military strikes to surveillance to product deliveries.

MALE Drones – A Medium Altitude Long Endurance (MALE) drone is a special type of drone often used for combat or reconnaissance purposes. This drone type is one classification among many kinds of drones found worldwide.

Quadcopter – A quadcopter is a drone that uses four different propellers to lift off the ground.

UAS – A UAS is an unmanned aircraft system, which includes both the unmanned aircraft itself along with the equipment necessary for operation of the aircraft.

UAV – A UAV is an unmanned aerial vehicle, which lacks certain safety systems found in manned vehicles and are typically operated via remote control.

Bibliography

ABC7 New York. “Invasion of Privacy? Debate Wages over Drone Use by Police in New York,” August 22, 2023. https://abc7ny.com/new-york-drones-invasion-of-privacy-police-departments/13685989/.

Ali.yusuf7. English: A Quadcopter Based on the Plus Design Configuration, with a Light Weight Aluminum Frame and Powerful 1000 Kva Motors. December 3, 2014. Own work. https://commons.wikimedia.org/wiki/File:Quadcopter_-_Plus_Design.JPG.

“Allocation of Agenda Items to the First Committee.” United Nations General Assembly. Accessed August 11, 2024. https://documents.un.org/doc/undoc/gen/n23/320/16/pdf/n2332016.pdf.

author, Unknown authorUnknown. English: Aircraft and Balloons Used by Some of the Air Pioneers Who Were Contemporary With Samuel Franklin Cody. Pre 1914. http://media.iwm.org.uk/iwm/mediaLib//13/media-13780/large.jpg This photograph RAE-O 870 comes from the collections of the Imperial War Museums. https://commons.wikimedia.org/wiki/File:Ruston,_Proctor_Radio_controlled_target_aircraft_RAE-O870.jpg.

“Autonomous and Remotely Operated Systems | Office of Counter-Terrorism.” Accessed August 29, 2024. https://www.un.org/counterterrorism/autonomous-and-remotely-operated-systems.

Bennett, Wells C. “Civilian Drones, Privacy, and the Federal-State Balance.” Brookings, March 9, 2022. https://www.brookings.edu/articles/civilian-drones-privacy-and-the-federal-state-balance/.

Burns, John F. “A NATION CHALLENGED: THE MANHUNT; U.S. Leapt Before Looking, Angry Villagers Say.” The New York Times, February 17, 2002, sec. World.

https://www.nytimes.com/2002/02/17/world/a-nation-challenged-the-manhunt-us-leapt-before-looking-angry-villagers-say.html.

Digital Trends. “The History of Drones in 10 Milestones,” September 11, 2018. https://www.digitaltrends.com/cool-tech/history-of-drones/.

“Disarmament and International Security (First Committee).” United Nations. Accessed August 11, 2024. https://www.un.org/en/ga/first/.

Drone Wars UK. “Who Has Armed Drones?,” February 4, 2019. https://dronewars.net/who-has-armed-drones/.

Dronemade. “Dronemade | Country Drone Laws 2024 | World Map.” Accessed August 29, 2024. https://www.drone-made.com/drone-laws.

“Drones.” UNICEF, n.d. https://www.unicef.org/innovation/drones.

“Drones for Firefighting.” Accessed August 29, 2024. https://www.skydio.com/solutions/public-safety/fire-fighting-drones/.

Drones For Good Worldwide. “DronesForGood - Worldwide | Donate Today To Save Lives.” Accessed August 29, 2024. https://dronesforgoodworldwide.org/.

“First Drone Crash with a Commercial Aircraft in Canada Triggers Safety Review and Possible New Rules.” EDI Weekly: Engineered Design Insider, June 21, 2017. https://www.ediweekly.com/first-drone-crash-commercial-aircraft-canada-triggers-safety-review-possible-new-rules/.

"High-Level Meetings of the 78th Session." United Nations. Accessed August 11, 2024. https://www.un.org/en/ga/78/meetings/.

"How Decisions Are Made at the UN." United Nations. Accessed August 11, 2024. https://www.un.org/en/model-united-nations/how-decisions-are-made-un#:~:text=Given%20the%20dramatic%20increase%20in,possible%20implementation%20of%20GA%20decisions.

"Kettering Aerial Torpedo 'Bug.'" National Museum of the United States Air Force, n.d. https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/198095/kettering-aerial-torpedo-bug/.

Lushenko, Paul. "The Moral Legitimacy of Drone Strikes: How the Public Forms Its Judgments." Texas National Security Review, March 3, 2023. https://tnsr.org/2022/11/the-moral-legitimacy-of-drone-strikes-how-the-public-forms-its-judgments/.

Markert, Francis. "Drone Rules and Laws in Morocco - Current Information and Experiences." Drone Traveller, February 25, 2018. https://drone-traveller.com/drone-laws-morocco/.

McNabb, Miriam. "All SIM Cards Are Not the Same: The Risks of Using Consumer SIM Cards for Drone Operations." DRONELIFE, January 16, 2023. https://dronelife.com/2023/01/16/all-sim-cards-are-not-the-same-the-risks-of-using-consumer-sim-cards-for-drone-operations/.

"Medium Altitude Long Endurance - an Overview | ScienceDirect Topics." Accessed August 29, 2024. https://www.sciencedirect.com/topics/engineering/medium-altitude-long-

endurance#:~:text=2.2%20Based%20on%20Altitude%20and%20Range&text=NATO%3A%20UAVs%20with%20an%20altitude,range%20less%20than%20200%20km.

"Mykolayivka, Ukraine (July 19, 2017) a U.S. Marine with Black Sea Rotational Force 17.1 Launches an Unmanned Aerial Vehicle during Exercise Sea Breeze 2017 in Mykolayivka." rawpixel. Accessed September 1, 2024. https://www.rawpixel.com/image/3393500/free-photo-image-drone-aerial-vehicle-armored.

p-themes. "Morocco Drone Laws." UAV Systems International. Accessed August 29, 2024. https://uavsystemsinternational.com/pages/morocco-drone-laws.

rshaffer. "A Not-So-Short History of Unmanned Aerial Vehicles (UAV)." Consortiq, June 10, 2020. https://consortiq.com/uas-resources/short-history-unmanned-aerial-vehicles-uavs.

"The Security Council." Flickr, September 2, 2024. https://www.flickr.com/photos/un_photo/24320174321.

"Top 10 Commercial Uses For Drones | Inspired Flight Technologies." Accessed August 29, 2024. https://www.inspiredflight.com/news/top-10-commercial-uses-for-drones.php.

UAV Coach. "Drone Laws in Singapore | UAV Coach (2023)." Accessed August 29, 2024. https://uavcoach.com/drone-laws-singapore/.

"Using Drones to Deliver Critical Humanitarian Aid | WFP Drones." Accessed August 29, 2024. https://drones.wfp.org/updates/using-drones-deliver-critical-humanitarian-aid.

Wang, Ning, Markus Christen, and Matthew Hunt. “Ethical Considerations Associated with ‘Humanitarian Drones’: A Scoping Literature Review.” Science and engineering ethics, August 3, 2021. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8330183/.

“WFP Drones,” June 25, 2024. https://drones.wfp.org/.

“What Is the Definition of Recreational or Hobby Use of a UAS or Drone?” Federal Aviation Administration. Accessed September 1, 2024. https://www.faa.gov/faq/what-definition-recreational-or-hobby-use-uas-or-drone#:~:text=Recreational%20or%20hobby%20UAS%20or%20drone%20use,the%20ordinary%2C%20dictionary%20definition%20of%20these%20terms.

“Workings of the General Assembly.” United Nations. Accessed August 11, 2024. https://www.un.org/en/ga/.

Topic B: Cyberwarfare

Statement of the Problem

Cyberwarfare is a concern because of a lack of governance on a national and international level. This stems from a lack of clear definition, the anonymity inherent to cyberattacks (which makes it hard to pin down the perpetrators and the intent of the attack), and the novelty of cyberwarfare as a concept. The following sections will outline the (loose) definition of cyberwarfare and will discuss the specific issues surrounding it. Aspects of anonymity as it relates to cyberattacks will not be discussed in this section, but will be discussed in the "History of the Problem" section further.

What is Cyberwarfare?

Defining cyberwarfare is difficult simply due to the lack of consensus on what it even is, or how it functions within the larger scope of the internet. Prior to delving into the exact definition of cyberwarfare, it is helpful to start by understanding **cyberspace**, which is already very vaguely defined. Looking at an assortment of texts, from government manuscripts to academic authors and even fiction writers to extract what is meant when the word is used colloquially, cyberspace generally seems to refer to a separate domain defined by the connections between computers that involves storing and modifying information.[45] It should be noted that this clarification still doesn't give concrete specifications to what cyberspace entails. For the purpose of the rest of the background guide, cyberspace should be thought of as the abstract–meaning existing only as a thought or idea and not concrete–domain where computers communicate to exchange information.

[45] Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, *Cyberpower and National Security*, Potomac Books, 2009.

Robinson et al. (2014) constructs a definition for cyberwarfare following a literature review of other academic sources that try to do the same, and they come to the conclusion that it can be defined as a combination of a cyberattack, which is an effort by an individual or group to breach a foreign information system, and the intent for achieving a military objective.

John Sandage, former Director of the Division for Treaty Affairs at the United Nations Office on Drugs and Crime, speaks during a panel on cybersecurity and cybercrime.[46]

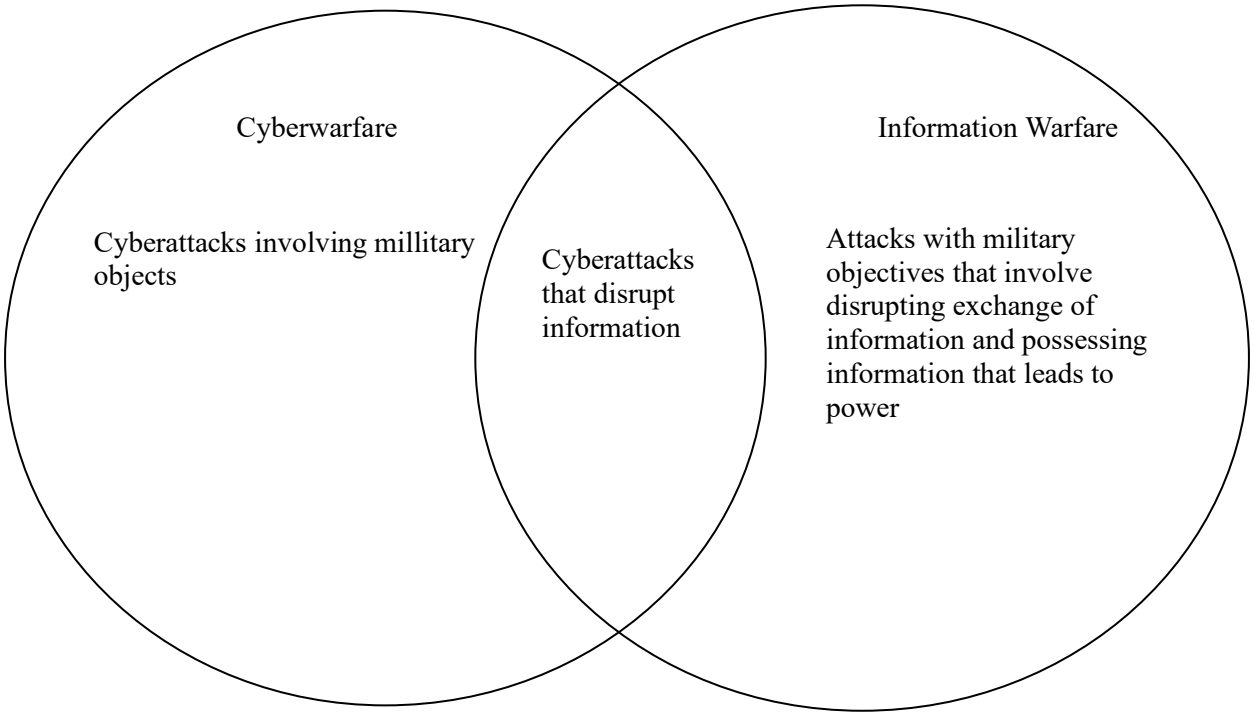
Cybercrime is the same as cyberwarfare in the sense that the act causes harm in cyberspace, but it differs in the intention of the act itself as it is typically motivated by personal gain achieved through illegal means. Many events involving anonymous attacks can only be categorized as either cyberwarfare or cybercrime by understanding the intent of the attack, which ultimately is not so easy to decipher.

---

[46] "High Level Panel on Cybersecurity and Cybercrime," Flickr, September 3, 2024, https://www.flickr.com/photos/unisgeneva/6796010553.

Information Warfare

Information warfare is another form of warfare that is related to cyberwarfare, but doesn't encompass it in its entirety.[47] This can best be understood using a Venn diagram, shown below. Information warfare mainly involves disrupting sources of information and gaining access to information that can lead to power. It is important to note that the definitions of these terms aren't especially concrete, as previously mentioned, but it is important to understand them as completely as possible to guide discussion of these topics.



The similarities and differences between cyberwarfare and information warfare.

Infrastructure Risks & Legal Structure of Cyberwarfare

There are two core problems that the international community faces in regard to cyberwarfare: issues protecting critical **infrastructure** against cyberattacks with a lack of legislation promoting its protection, and a lack of international legislation governing cyberwarfare. According to sources such as the International Energy

[47] Michael Robinson, Kevin Jones, and Helge Janicke, "Cyber Warfare: Issues and Challenges," Computers & Security 49 (March 1, 2015): 70–94, https://doi.org/10.1016/j.cose.2014.11.007.

Agency, cyberattacks on national infrastructure more than doubled following 2020,[48] especially as geopolitical issues around the world have resulted in a heightened focus on cyber risks.

Since the 2000s, there has been a significant rise in the number of nations that have the capabilities as well as the motivation to conduct cyberattacks, according to the Institute for Security Technology Studies at Dartmouth.[49] For example, training for electronic warfare was implemented in China as part of its military exercises, Indian authorities shifted military priorities in 1998 to embrace electronic warfare, and an article in the Bulletin of Atomic Scientists outlines numerous occasions where the U.S. military heavily considered conducting cyberattacks according to various journalistic sources.[50] Furthermore, every few years a new type of vulnerability that was never accounted for in cyber infrastructure seems to be uncovered, with researchers at Georgia Tech in February of 2024 discovering vulnerabilities that could allow malware to disrupt industrial systems–like the infrastructure that brings electricity into our homes.[51] Ultimately, there is a large lack of grassroots efforts to maintain cybersecurity in many nations, which could leave some countries far more vulnerable to acts of cyberwarfare than others.

In large part, the way in which international law deals with cyberwarfare is by applying existing international law to cyberspace. The United Nations Office on Drugs and Crime (UNODC) uses the **Tallinn Manual** as an example of how international law can be and has been used to regulate cyberwarfare, but this manual isn't a legally binding document and only provides resources for ways in which legal experts can

---

[48] "Why the World Needs a New Cyber Treaty for Critical Infrastructure," accessed August 11, 2024. https://carnegieendowment.orgundefined?lang=en.

[49] Charles Billo and Welton Chang, "CYBER WARFARE AN ANALYSIS OF THE MEANS AND MOTIVATIONS OF SELECTED NATION STATES," Institute for Security Technology Studies at Dartmouth College, November 2004, www.cryptome.org/2013/07/cyber-war-racket-0003.pdf.

[50] Max Smeets, "A US History of Not Conducting Cyber Attacks," Bulletin of the Atomic Scientists 78, no. 4 (July 4, 2022): 208–13, https://doi.org/10.1080/00963402.2022.208738

[51] "Critical Infrastructure Systems Are Vulnerable to a New Kind of Cyberattack," February 29, 2024. https://coe.gatech.edu/news/2024/02/critical-infrastructure-systems-are-vulnerable-new-kind-cyberattack.

understand these issues. However, even the manual admits that extensions of existing international law to cyberwarfare don't cover many forms of cyberattacks. For example, a review of the manual points out the manual's admission that **cyberespionage** during peacetime doesn't violate the existing law, even if certain methods of cyberespionage could violate these laws.[52] Interestingly, however, the authors of the manual suggest that the right to privacy as it relates to personal data could be protected under existing laws.[53]

One important piece of existing legislation that experts within the cyberwarfare space believe can potentially be applied to cyberwarfare is the **Law of Armed Conflict (LOAC)**. This legislation regulates the actions of participants in armed conflicts to ensure that the impacts of the conflict on neighboring regions is minimized and that civilians are at most minimally affected. The Military Law Review, for example, brings up the point that the LOAC is applied when there is a "use of force, regardless of the weapons employed" which raises the question as to whether or not computers are considered a "force" that can be used.[54] The authors of the Review agree that the norm is for the LOAC to apply, but point out that applying the law to cyberspace can be difficult since there is no agreed-upon definition of cyberspace acts of war. Additionally, there is also no existing treaty or similar document that draws clear similarities between cyberspace acts of war and traditional acts of war, in which case perhaps the LOAC could be applied.

So what does this context regarding international law and its application mean for how this committee should attempt to address cyberwarfare? The context is meant to show the extent of the lack of clarity when it comes to how cyberwarfare is legislated. There are no international treaties that govern or define cyberwarfare and

---

[52] Eric T. Jense, "THE TALLINN MANUAL 2.0: HIGHLIGHTS AND INSIGHTS," Georgetown Journal of International Law, n.d., https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf.

[53] Ibid.

[54] Gary D. Solis, "Cyber Warfare," Military Law Review 219 (2014): 1., https://heinonline.org/HOL/Page?handle=hein.journals/milrv219&id=7&div=&collection=.

cybercrime, especially when blame is hard to place when cyberattacks are anonymous. Outside of dealing with the harms and risks inherent to cyberwarfare as detailed in the beginning of the section, delegates will need to also contend with what the future of international law will look like given the rapid emergence of the cyberspace and the complications that come with it.

History of the Problem

As with any topic of interest, discussing the issues surrounding cyberwarfare will be easier once we discuss the history of cyberwarfare and its uses. However, this comes with the caveat that with most incidents of cyberwarfare, assigning culpability or motive to most if not all of these incidents is not possible without some level of speculation. We hope to stray away from these discussions, and rather bring light to aspects of cyberwarfare that need to be considered by delegates and are exemplified by the incidents detailed below.

2007 Cyberattacks on Estonia

Estonian history following 1939 was defined by its relationship with the neighboring USSR, starting in August of that year when Nazi Germany and the Soviet Union signed the Molotov-Ribbentrop Pact,[55] which was a non-aggression pact that was also meant to divide the states in Central and Eastern Europe between the "spheres of influence" of Nazi Germany and the USSR. Following this treaty, the USSR established military bases in Estonia in late 1939, and then later annexed Estonia in 1940. Following the annexation, the USSR established a repressive regime over the course of two separate occupations, arresting many high-ranking individuals and deporting thousands of "enemies of the state" to remote parts of the Soviet Union. Following the annexation, Estonia gained independence in 1991 and was admitted to the UN.

[55] Yaël Ronen, *Transition from Illegal Regimes under International Law*, Cambridge University Press, 2011.

Soviet troops in 1939 moving into military bases in Estonia after the Molotov-Ribbentrop Pact was ratified.[56]

An important vestige of the Soviet era in Estonia is the "Bronze Soldier", a Soviet WWII memorial which was controversial due to differences in interpretations of the war by different political groups.[57] The memorial was moved–which also involved the **exhumation** and identification of the remains of Soviet soldiers–which led to riots.

Amidst this conflict, a three-week-long wave of cyberattacks were levied against Estonia, targeting media sources, banks, and even the parliament. The Guardian at the time called it the "first known instance of such an assault on a state",[58] referring to the use of cyberspace to conduct military attacks. These attacks limited Estonians'

---

[56] "File:Red Army Entering into Estonia in 1939.Jpg - Wikipedia," October 18, 1939, https://commons.wikimedia.org/wiki/File:Red_Army_entering_into_Estonia_in_1939.jpg.

[57] Der Spiegel, "Deadly Riots in Tallinn: Soviet Memorial Causes Rift between Estonia and Russia," April 27, 2007, sec. International, https://www.spiegel.de/international/europe/deadly-riots-in-tallinn-soviet-memorial-causes-rift-between-estonia-and-russia-a-479809.html.

[58] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," The Guardian, May 17, 2007, sec. World news, https://www.theguardian.com/world/2007/may/17/topstories3.russia.

access to their money, disrupted communication between government officials as well as civilians, and exposed the possibility for cyberattacks to cause long-lasting damage.[59] NATO's Strategic Communications Center of Excellence also noted that the cyberattacks' effects were also psychological in nature, as they reduced people's trust in their government to protect them from cyberattacks and made apparent the fact that these cyberattacks could have been far deadlier due the large amount of vulnerabilities.[60] Following these attacks, NATO dispatched experts to support Estonia's cyber defenses. Many countries started to follow suit by working to strengthen their cyber defenses.

The Guardian, however, noted that officials were careful not to pin accusations on Russia,[61] since this form of military action was unprecedented and wasn't yet defined as warfare. Furthermore, there was no concrete evidence that the perpetrators were committing government-sanctioned military action; all they knew was that the attacks came from Russian **IP addresses.**[62] To complicate the situation further, it is generally accepted among experts that malicious third party groups often bandwagon following a cyberattack, so even if the Russian military was involved, it would have been unclear who was responsible for what attack. In this case, NATO's Article 5, which guarantees NATO members will defend each other following military attacks on a member state, was not triggered because there was no loss of life similar to that of traditional military actions.[63]

This event is important to consider when understanding the problems and the scope of cyberwarfare as an issue. Following these attacks, it became pivotal for states to decide when cyberattacks are acts of war, with the

---

[59] "2007 Cyber Attacks on Estonia," NATO Strategic Communications Centre of Excellence, n.d., https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf.

[60] Ibid.

[61] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia."

[62] BBC News, "How a Cyber Attack Transformed Estonia," April 27, 2017, sec. Europe, https://www.bbc.com/news/39655415.

[63] Ibid.

chair of NATO's military committee stating this past year that a cyberattack can trigger Article 5 and be considered as an act of war.[64] These attacks were the catalyst for the increase in consideration of cyberattacks as potential forms of warfare.

Russo-Georgian War of 2008

The Russo-Georgian War is another unprecedented incident of cyberwarfare as it was the first time that cyberattacks coincided with traditional military action. The incidents of interest started with information warfare that used media outlets to spread disinformation and accusations of spreading disinformation to sway public opinion. Furthermore, media campaigns were utilized to discredit claims from the other side, which included the release of intercepted phone conversations, and outside journalists were restricted to the region of South Ossetia, an autonomous republic in Georgia.[65] During the war, Georgian government websites were shut down by hackers,[66] and some websites were defaced. These **distributed denial-of-service (DDoS)** attacks were attributed to a Russian hacker group, but experts pointed out that the attacks showed similarities to the 2007 cyberattacks in Estonia.[67] It's important to also note that the Russian news agency RIA Novosti was also targeted by a cyberattack.

Information warfare here, in tandem with traditional warfare, allowed both countries to gain victories in ways that would be impossible with traditional warfare. Al Jazeera noted that Georgia's propaganda campaign

---

[64] The International Institute for Strategic Studies, "IISS Shangri-La Dialogue 2024 | Special Session 5: AI, Cyber Defence and Future Warfare," accessed August 22, 2024. https://www.youtube.com/watch?v=qveCFae6rEQ&t=2795s.

[65] Al Jazeera, "Media War Flares over S Ossetia," accessed August 22, 2024, https://www.aljazeera.com/news/2008/11/24/media-war-flares-over-s-ossetia.

[66] Asher Moses, "Georgian Websites Forced Offline in 'Cyber War'," The Sydney Morning Herald, August 12, 2008, https://www.smh.com.au/technology/georgian-websites-forced-offline-in-cyber-war-20080812-gdsqac.html.

[67] ZDNET, "Coordinated Russia vs Georgia Cyber Attack in Progress," accessed August 22, 2024, https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/.

succeeded in its ability to reach the West by always maintaining media access to English speaking ministers,[68] but the New York Times pointed out later in 2014 that Russia's campaign was instrumental in maintaining high approval ratings for then president Dmitri A. Medvedev.[69] The cyberattacks in this example were harmful to Georgia, but most importantly they allowed Russia to catch up in the information war that was waging by slowing Georgian news reporting.

This incident of cyberattacks in tandem with other forms of warfare exemplify the fact that–although cyberattacks are inherently very dangerous–the effects of cyberattacks can often increase the effectiveness of other forms of warfare.

Shadow Network

In 2009, a report was published discussing one of two espionage operations based out of China that primarily infected computer systems in the office of the Dalai Lama,[70] but infected many computer networks belonging to the Indian Government. The report was published by the data and artificial intelligence consultancy firm SecDev, which at the time was collaborating with a lab at the University of Toronto on a project called the Information Warfare Monitor, which was focused on tracking the emergence of cyberspace. Through this project, they were able to recover thousands of emails and documents that were compromised. This included emails from the Dalai Lama's office and classified reports on the security of Indian states and military documents. However, according to the findings of the authors of the report, computers from all across the world were compromised or infected by the malware, showing how some cyber incidents can have devastating and far-reaching consequences.

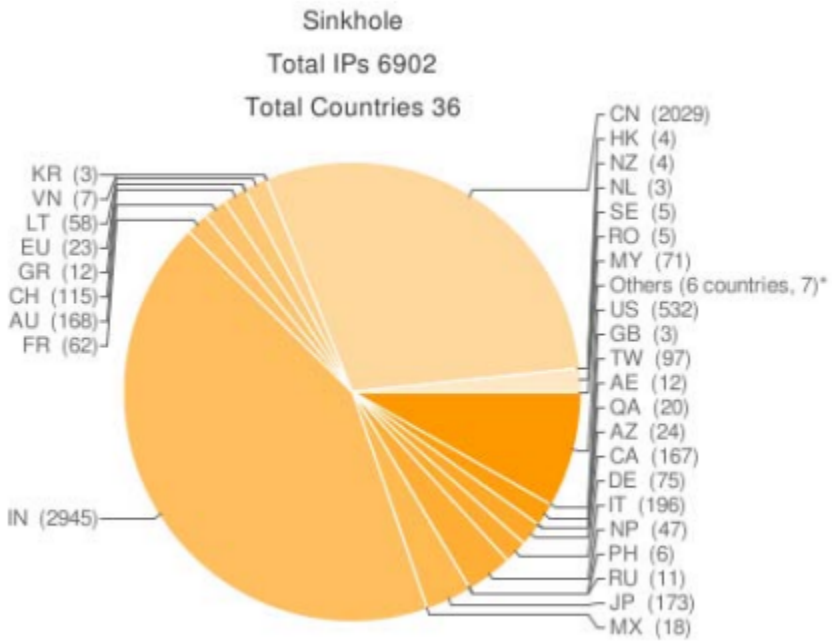
---

[68] Al Jazeera, "Media War Flares over S Ossetia," accessed August 22, 2024, https://www.aljazeera.com/news/2008/11/24/media-war-flares-over-s-ossetia.

[69] Olesya Vartanyan and Ellen Barry, "If History Is a Guide, Crimeans' Celebration May Be Short-Lived," The New York Times, March 18, 2014, sec. World, https://www.nytimes.com/2014/03/19/world/europe/south-ossetia-crimea.html.

[70] "Shadows in the Clouds: Investigating Cyber Espionage 2.0," The SecDev Group, n.d., https://www.nartv.org/mirror/shadows-in-the-cloud.pdf.

Furthermore, this case is important to showcase that cyberwarfare can be highly effective in its use by states that want to undermine or attack political groups that oppose them, as these attacks can rarely be traced back to the government itself.



The graph above shows the number of infected IPs the authors of the 2009 report were able to discern and the countries they originated from.[71]

Stuxnet

In a similar vein to the previously mentioned cyberattacks, Stuxnet is also one of the first of its kind in that it is one of the first acts of cyberwarfare that caused physical damage across international borders, once again bringing into question what counts as an act of war. In addition, it also challenges a previously held assumption

[71] Ibid.

that cyberwarfare makes warfare fairer between more and less powerful countries as it displays how powerful countries can take advantage of this medium of warfare very effectively.[72]

Between 2006 and 2008, many UNSC resolutions demanded Iran suspend its nuclear processing, but Iran refused to cooperate fully, citing that the processing would be necessary to meet its future energy requirements.[73] Following these events, Iranian news sources reported that a malware was affecting many industries across Iran, but not recognizing specific sites.[74] Experts believed that this malware–Stuxnet–was likely aimed to disrupt the opening of a new nuclear power plant. Independent news sources would later claim in 2012 that this attack wasn't just random malware, but a targeted cyberattack headed by the United States and Israel to slow down Iran's nuclear progress.[75] Delegates should use this cyber incident to consider how incidents of cyberwarfare can have far-reaching effects beyond just the cyberspace.

---

[72] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," Security Studies 22, no. 3 (July 2013): 365–404, https://doi.org/10.1080/09636412.2013.816122.

[73] Ibid.

[74] The Associated Press, "Iran's Nuclear Agency Trying to Stop Computer Worm," September 25, 2010, https://archive.ph/20100925234352/http://www.nytimes.com/aponline/2010/09/25/world/middleeast/AP-ML-Iran-Cyber-Attacks.html?_r=1#selection-431.0-431.50.

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

The nuclear power plant that opened in 2010 which is claimed to have been the target of Stuxnet.[76]

2016 U.S. Election Interference

This last historical incident of cyberwarfare differs from the previous incidents in its goals and results while at the same time showcases the extremes in the governmental mistrust (as discussed in the 2007 Estonia section) created by cyberattacks. The election interference discussed in this subsection comes in two forms: voter database hacks and leaks of private emails within the Democratic National Convention.

The Senate Intelligence Committee's 2019 report found that state election infrastructure across all states was in some way hacked by what they claimed were agents of Russian intelligence in 2016.[77] They also noted that there were no findings suggesting that votes themselves were changed or manipulated, but they did find that the

---

[76] Imagebank, Paolo Contri/IAEA. English: A View from the Busher Nuclear Power Plant in Iran, September 29, 2000, Flickr, https://commons.wikimedia.org/wiki/File:Bushehr_NPP_%2804710033%29.jpg.

[77] "U.S. Senate Select Committee on Intelligence, Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 1: Russian Efforts Against Election Infrastructure With Additional Views," Washington, D.C.: U.S. Senate, 2019. accessed January 10, 2020, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

information of these voters was vulnerable and was stolen. The damages of the incident are somewhat clear, as the report determined that voter information was stolen and the lack of security around the election was exposed, but what is less clear is the effect this had on the American population and its trust in the elections as a whole. The press surrounding the election interference scandal continues to affect discussions around election integrity to this day, with news outlets continuing to speculate on Russian involvement in U.S. elections in 2024.

Once again, in the summer of 2016, hackers alleged to be a part of the Russian intelligence agency hacked into the emails of key Democratic National Convention staff members that showed details of DNC interactions with the Hillary Clinton and Bernie Sanders presidential campaigns, which included emails from staff members of the DNC ridiculing the Sanders campaign and discussing their favor towards Clinton's campaign. Note also that these leaks included many documents that revealed people's Personal Identifiable Information, allowing for identity fraud to occur, and would also reveal classified information with the potential to compromise national security.[78] As a result, many people lost trust in the Democratic Party, especially those who supported the Sanders campaign, and the leaks would become one of the most important points of debate in the 2016 election.

These incidents had the effect of essentially changing the conversation surrounding the election in its entirety. Delegates should note that even without actively attacking cyber infrastructure or actively changing the reporting of information using their own media outlets, countries can utilize cyberwarfare to create a large-scale distrust in institutions within populations of other countries.

---

[78] Andrea Peterson, "Snowden and WikiLeaks Clash over Leaked Democratic Party Emails," The Washington Post, July 28, 2016, https://www.washingtonpost.com/news/the-switch/wp/2016/07/28/a-twitter-spat-breaks-out-between-snowden-and-wikileaks/.

Past Actions

Early UN Resolutions

Since at least the 1990s, the UN General Assembly has drafted numerous different resolutions regarding cyberattacks. Many of these early resolutions, such as Resolution 55/63, discussed cybercrime and cybersecurity as its main focus.[79] These documents emphasized reducing misuse of information technology for criminal reasons. One of the earliest resolutions to broach the topic of cyberwarfare rather than simply cybersecurity was a draft resolution introduced by the Russian Government on September 23, 1998. This resolution, as described by Tim Maurer in the discussion paper "Cyber Norm Emergence at the United Nations",[80] was one of the first attempts at a "cyber arms control treaty", which differed from the position of the U.S. at the time which was that cyberwarfare should be regulated in the exact same way that traditional warfare was. This resolution was passed on January 4, 1999, and importantly mentions the military potential of cyberspace for the first time and strongly emphasizes the need to prevent cybercrime and cyberterrorism.

Progress Towards a Cyberwarfare Treaty

Over the next few years from around the 2000s to 2008, there was a period of resolutions being introduced for the purpose of creating a cyber arms treaty, but subsequently often being opposed by the U.S. and other European countries.[81] These states were skeptical as such a treaty had the potential to limit freedom of information and potentially control mass media. Furthermore, experts at the Ministry of Defense of the Russian Federation also saw the U.S.'s lack of support as caused by the fact that it was–at this point in history–the leader

---

[79] "Resolution Adopted by the General Assembly [on the Report of the Third Committee (A/55/593)] 55/63. Combating the Criminal Misuse of Information Technologies," UN General Assembly, January 22, 2001, https://documents.un.org/doc/undoc/gen/n00/563/17/pdf/n0056317.pdf.

[80] "Cyber Norm Emergence at the United Nations—An Analysis of the UN's Activities Regarding Cyber-Security | The Belfer Center for Science and International Affairs," August 14, 2023, https://www.belfercenter.org/publication/cyber-norm-emergence-united-nations-analysis-uns-activities-regarding-cyber-security.

[81] Ibid.

in the cyberwarfare field. Following an administration change, in 2009 the U.S. sought to improve relations with Russia and the UN, and thus co-sponsored Resolution 65/41, drafted by Russia in 2010, a resolution which many considered to be a significant step towards a cyberwarfare treaty.[82] Most importantly, the resolution established a "group of governmental experts ... to study existing and potential threats in the sphere of information security."[83] This group, known as a GGE or "Group of Governmental Experts", would go on to publish 3 cybersecurity reports, with the first coming out in 2013. It is now important to analyze the recommendations made by the GGE in their reports as the more recent Resolution 77/37 states that these conclusions are vital to maintaining security.[84]

The reports clarify that states should not knowingly allow their territory to be used for "internationally wrongful acts using [information & communication technology]",[85] which includes requiring states to take reasonable action to address such a situation. Furthermore, they suggest that states should protect their own critical infrastructure to ensure they suffer at most minimal damage from cyberattacks. There have also been multiple uses of organizational platforms, including the United Nations Institute for Disarmament Research (UNIDIR), which helped conduct research and host cybersecurity discussions, and the International

---

[82] Ibid.

[83] "Resolution Adopted by the General Assembly on 8 December 2010 [on the Report of the First Committee (A/65/405)] 65/41. Developments in the Field of Information and Telecommunications in the Context of International Security ." United Nations General Assembly, January 11, 2011, https://documents.un.org/doc/undoc/gen/n10/515/00/pdf/n1051500.pdf.

[84] "Resolution Adopted by the General Assembly on 7 December 2022 [on the Report of the First Committee (A/77/380, Para. 11)] 77/37. Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security." United Nations General Assembly, December 12, 2022, https://documents.un.org/doc/undoc/gen/n22/737/71/pdf/n2273771.pdf.

[85] "Group of Governmental Experts – UNODA," accessed August 28, 2024, https://disarmament.unoda.org/group-of-governmental-experts/.

Telecommunications Union, which launched the Global Cybersecurity Agenda and developed model legislation for member states to follow.[86]

Michele Markoff, former U.S. Senior Policy Advisor in the Office of the Secretary for Cyber-Security Affairs, speaks at a UNIDIR cybersecurity conference in 2012.[87]

[86] "Cyber Norm Emergence at the United Nations—An Analysis of the UN's Activities Regarding Cyber-Security | The Belfer Center for Science and International Affairs," August 14, 2023, https://www.belfercenter.org/publication/cyber-norm-emergence-united-nations-analysis-uns-activities-regarding-cyber-security.

[87] Geneva, United States Mission, UNIDIR Cyber Conference, November 9, 2012, https://www.flickr.com/photos/us-mission/8169779889/.

Possible Solutions

Earlier sections within this topic make clear that the debate of cyberwarfare is rather large in scope. This requires delegates to address multiple subtopics, including but not limited to cybersecurity technology, in order to prevent harm caused cyberattacks, legislation, in order to clarify what constitutes cyberwarfare and to create policies to defend against it, and importantly enforcement of the legislation delegates come up with. Delegates should consider the general ideas below when brainstorming their own solutions.

Developing a "Cyber Treaty"

A common policy proposition suggested is the creation of a cyber treaty, which was also discussed in the "Past Actions" section.[88] The ways in which different parties imagine the treaty can often differ significantly. The German Council on Foreign Relations suggests constructing a treaty that is limited in scope, where it would only guarantee the protection of a country's critical infrastructure, but yet the treaty should still be hard to undermine. One of the members of the Council, Dr. Valentin Weber, notes that even without considering whether getting states to agree to the declaration is realistic, ensuring that the terms of the treaty cannot be undermined may be difficult.[89] In a Carnegie Endowment for International Peace article, the authors also suggest the creation of a cyber treaty with the goal of protecting critical infrastructure.[90] Rather than fully ignoring existing international law, they suggest creating a new framework with additional obligations for countries and specifically prohibiting specific types of cyberattacks. This differs from existing proposals since ideally the treaty wouldn't support the political agendas of specific countries nor would it be limited in the scope of its actions.

---

[88] "Why the World Needs a New Cyber Treaty for Critical Infrastructure," accessed August 11, 2024, https://carnegieendowment.orgundefined?lang=en.

[89] "How German (Cyber)Diplomacy Can Strengthen Norms in a World of Rule-Breakers | DGAP," accessed August 28, 2024, https://dgap.org/en/research/publications/how-german-cyberdiplomacy-can-strengthen-norms.

[90] "Why the World Needs a New Cyber Treaty for Critical Infrastructure," accessed August 11, 2024, https://carnegieendowment.orgundefined?lang=en.

Treaties or declarations like those described above seem like simple solutions to address cyberwarfare, but largely lack popularity. As noted in the "Past Actions" section, the United States from 2005-2008 was staunchly opposed to such agreements due to concerns regarding freedom of expression. Delegates should consider the types of agreements that will be appropriate to address cyberwarfare, if any agreement is necessary at all, and the mechanisms by which compliance can be guaranteed.

Enforcement

Enforcement of cyberwarfare legislation is lacking. For the most part, due to the anonymous nature of cyberattacks, enforcing international cyberwarfare law can be difficult or even near impossible. Delegates should consider when enforcement is necessary and how this enforcement should be conducted. An example from the Georgetown Journal of International Affairs suggests the creation of a cyber enforcement arm of the UN that would be deployed to investigate cyberattacks, protect critical infrastructure, and function analogously to the UN Peacekeepers, but in the cyber setting.[91]

[91] Walter Dorn, "Cyberpeacekeeping: A New Role for the United Nations?," Georgetown Journal of International Affairs 18 (2017): 138, https://heinonline.org/HOL/Page?handle=hein.journals/geojaf18&id=399&div=&collection=.

Bloc Positions

Due to the rapidly evolving nature of cyberspace over the past few decades–with an increase in both its capacity and the global understanding of it–the dais believes that historical bloc positions do not need to be adhered to. To better understand different country positions over the history of the UN's involvement in cybercrime, referring to the "Past Actions" section can be a good place to start. Outlined below are some perspectives to consider when thinking through your own country's position. Delegates need not stick to the positions below, but will need to form their positions based on the country assigned.

Countries With Robust Digital Infrastructure

A common understanding of cyberwarfare is that countries with robust digital infrastructure are most affected by cyberwarfare. To some extent, this can be true. Many countries rely on computers for many parts of their critical infrastructure for vital resources, such as water and electricity. In addition, these countries also have the highest capacity for conducting cyberattacks while maintaining anonymity. These countries may therefore choose to be careful about agreements that could limit freedoms of their citizens and their use of cyberespionage.

Countries Without Robust Digital Infrastructure

Although it may seem that these countries are unaffected by cyberwarfare, states without robust digital security can be far more susceptible to cyberattacks and information leaks. This can mean that cyberattacks are not only harmful due to the damage they can cause to these types of countries' infrastructures, but they can also harm citizens' perceptions of their digital safety. These countries may be more inclined to support protective legislation to ensure security.

Glossary

Cyberespionage - A type of cyberattack involving an attempt to access confidential data, typically for economic or political gain.

Cyberspace - A domain where actions involving the connections between computers and storing and accessing information occurs.

Cyberwarfare - Cyberattacks conducted for military purposes.

Cyberattack - An act that causes damage to another entity within the cyberspace.

Distributed Denial-of-Service (DDoS) - An attack where a hacker disrupts typical internet traffic, making websites and other online services hard to connect to.

Exhumation - The act of digging up something buried, often corpses.

Infrastructure - Basic organizational structures that allow for a certain area, such as society or information technology, to function. Examples of infrastructure development include the power grid and highway systems.

IP Address - A unique number assigned to devices that connect to the internet.

Law of Armed Conflict (LOAC) - Legislation that defines rules of conduct for combatants in an armed conflict.

Tallinn Manual - An academic study focusing on how existing international law applies to cyberwarfare.

Bibliography

"IISS Shangri-La Dialogue 2024 | Special Session 5: AI, Cyber Defence and Future Warfare - YouTube." Accessed August 22, 2024. https://www.youtube.com/watch?v=qveCFae6rEQ&t=2795s.

"2007 Cyber Attacks on Estonia." NATO Strategic Communications Centre of Excellence, n.d. https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf.

Al Jazeera. "Media War Flares over S Ossetia." Accessed August 22, 2024. https://www.aljazeera.com/news/2008/11/24/media-war-flares-over-s-ossetia.

BBC News. "How a Cyber Attack Transformed Estonia." April 27, 2017, sec. Europe. https://www.bbc.com/news/39655415.

Billo, Charles, and Welton Chang. "CYBER WARFARE AN ANALYSIS OF THE MEANS AND MOTIVATIONS OF SELECTED NATION STATES." INSTITUTE FOR SECURITY TECHNOLOGY STUDIES AT DARTMOUTH COLLEGE, November 2004. www.cryptome.org/2013/07/cyber-war-racket-0003.pdf.

"Critical Infrastructure Systems Are Vulnerable to a New Kind of Cyberattack," February 29, 2024. https://coe.gatech.edu/news/2024/02/critical-infrastructure-systems-are-vulnerable-new-kind-cyberattack.

"Cyber Norm Emergence at the United Nations—An Analysis of the UN's Activities Regarding Cyber-Security | The Belfer Center for Science and International Affairs," August 14, 2023. https://www.belfercenter.org/publication/cyber-norm-emergence-united-nations-analysis-uns-activities-regarding-cyber-security.

Der Spiegel. “Deadly Riots in Tallinn: Soviet Memorial Causes Rift between Estonia and Russia.” April 27, 2007, sec. International. https://www.spiegel.de/international/europe/deadly-riots-in-tallinn-soviet-memorial-causes-rift-between-estonia-and-russia-a-479809.html.

Dorn, Walter. “Cyberpeacekeeping: A New Role for the United Nations?” Georgetown Journal of International Affairs 18 (2017): 138. https://heinonline.org/HOL/Page?handle=hein.journals/geojaf18&id=399&div=&collection=.

“File:Red Army Entering into Estonia in 1939.Jpg - Wikipedia,” October 18, 1939. https://commons.wikimedia.org/wiki/File:Red_Army_entering_into_Estonia_in_1939.jpg.

Geneva, United States Mission. UNIDIR Cyber Conference. November 9, 2012. Photo. https://www.flickr.com/photos/us-mission/8169779889/.

“Group of Governmental Experts – UNODA.” Accessed August 28, 2024. https://disarmament.unoda.org/group-of-governmental-experts/.

“High Level Panel on Cybersecurity and Cybercrime.” Flickr, September 3, 2024. https://www.flickr.com/photos/unisgeneva/6796010553.

“How German (Cyber)Diplomacy Can Strengthen Norms in a World of Rule-Breakers | DGAP.” Accessed August 28, 2024. https://dgap.org/en/research/publications/how-german-cyberdiplomacy-can-strengthen-norms.

Imagebank, Paolo Contri/IAEA. English: A View from the Busher Nuclear Power Plant in Iran. September 29, 2000. Flickr. https://commons.wikimedia.org/wiki/File:Bushehr_NPP_%2804710033%29.jpg.

Jensen, Eric T. “THE TALLINN MANUAL 2.0: HIGHLIGHTS AND INSIGHTS .” GEORGETOWN JOURNAL OF INTERNATIONAL LAW, n.d. https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf.

Kalhh. English: Cyberspace Battles Image. December 22, 2015. https://pixabay.com/illustrations/laptop-internet-reality-cyberspace-1104066/. https://commons.wikimedia.org/wiki/File:Cyberspace_battles.jpg.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. Cyberpower and National Security. Potomac Books, 2009.

Lindsay, Jon R. “Stuxnet and the Limits of Cyber Warfare.” Security Studies 22, no. 3 (July 2013): 365–404. https://doi.org/10.1080/09636412.2013.816122.

Moses, Asher. “Georgian Websites Forced Offline in ‘Cyber War.’” The Sydney Morning Herald, August 12, 2008. https://www.smh.com.au/technology/georgian-websites-forced-offline-in-cyber-war-20080812-gdsqac.html.

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

Peterson, Andrea. “Snowden and WikiLeaks Clash over Leaked Democratic Party Emails.” The Washington Post, July 28, 2016. https://www.washingtonpost.com/news/the-switch/wp/2016/07/28/a-twitter-spat-breaks-out-between-snowden-and-wikileaks/.

"Resolution Adopted by the General Assembly on 7 December 2022 [on the Report of the First Committee (A/77/380, Para. 11)] 77/37. Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security." United Nations General Assembly, December 12, 2022. https://documents.un.org/doc/undoc/gen/n22/737/71/pdf/n2273771.pdf.

"Resolution Adopted by the General Assembly on 8 December 2010 [on the Report of the First Committee (A/65/405)] 65/41. Developments in the Field of Information and Telecommunications in the Context of International Security." United Nations General Assembly, January 11, 2011. https://documents.un.org/doc/undoc/gen/n10/515/00/pdf/n1051500.pdf.

"Resolution Adopted by the General Assembly [on the Report of the Third Committee (A/55/593)] 55/63. Combating the Criminal Misuse of Information Technologies ." UN General Assembly, January 22, 2001. https://documents.un.org/doc/undoc/gen/n00/563/17/pdf/n0056317.pdf.

Robinson, Michael, Kevin Jones, and Helge Janicke. "Cyber Warfare: Issues and Challenges." Computers & Security 49 (March 1, 2015): 70–94. https://doi.org/10.1016/j.cose.2014.11.007.

Ronen, Yaël. Transition from Illegal Regimes under International Law. Cambridge University Press, 2011.

Shadows in the Clouds: Investigating Cyber Espionage 2.0. The SecDev Group, n.d. https://www.nartv.org/mirror/shadows-in-the-cloud.pdf.

Smeets, Max. "A US History of Not Conducting Cyber Attacks." Bulletin of the Atomic Scientists 78, no. 4 (July 4, 2022): 208–13. https://doi.org/10.1080/00963402.2022.2087380.

Solis, Gary D. “Cyber Warfare.” Military Law Review 219 (2014): 1. https://heinonline.org/HOL/Page?handle=hein.journals/milrv219&id=7&div=&collection=.

The Associated Press. “Iran’s Nuclear Agency Trying to Stop Computer Worm.” September 25, 2010. https://archive.ph/20100925234352/http://www.nytimes.com/aponline/2010/09/25/world/middleeast/AP-ML-Iran-Cyber-Attacks.html?_r=1#selection-431.0-431.50.

Traynor, Ian. “Russia Accused of Unleashing Cyberwar to Disable Estonia.” The Guardian, May 17, 2007, sec. World news. https://www.theguardian.com/world/2007/may/17/topstories3.russia.

Vartanyan, Olesya, and Ellen Barry. “If History Is a Guide, Crimeans’ Celebration May Be Short-Lived.” The New York Times, March 18, 2014, sec. World. https://www.nytimes.com/2014/03/19/world/europe/south-ossetia-crimea.html.

“Why the World Needs a New Cyber Treaty for Critical Infrastructure.” Accessed August 11, 2024. https://carnegieendowment.orgundefined?lang=en.

ZDNET. “Coordinated Russia vs Georgia Cyber Attack in Progress.” Accessed August 22, 2024. https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/.