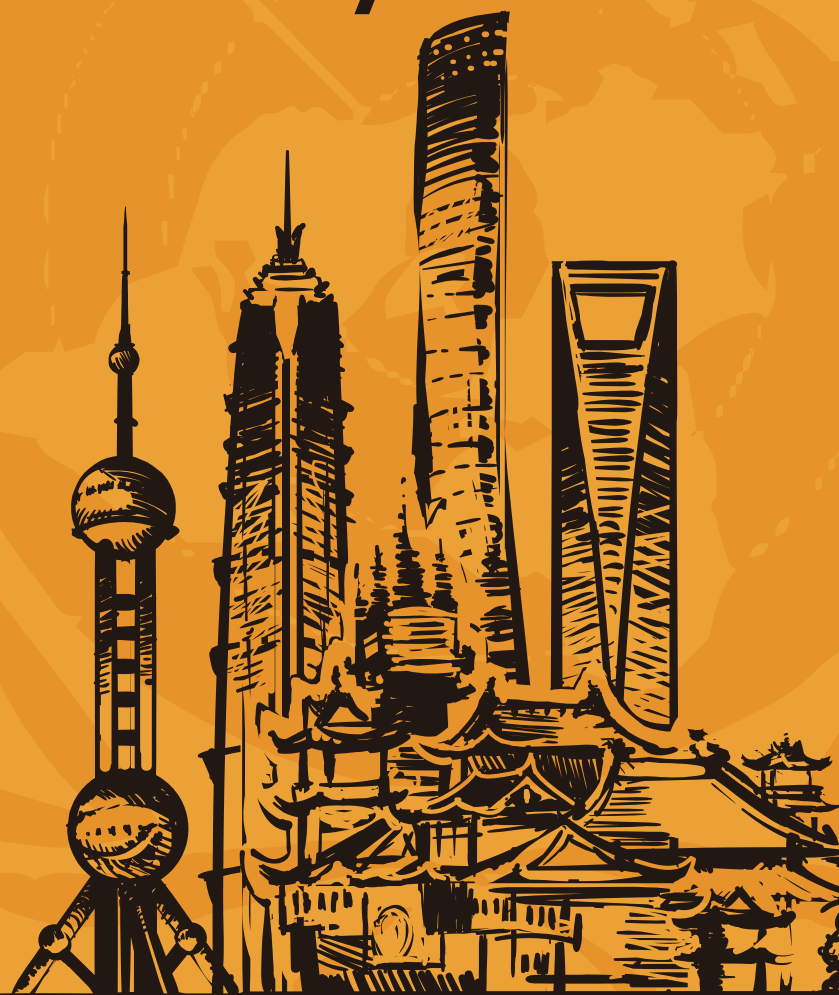
2025

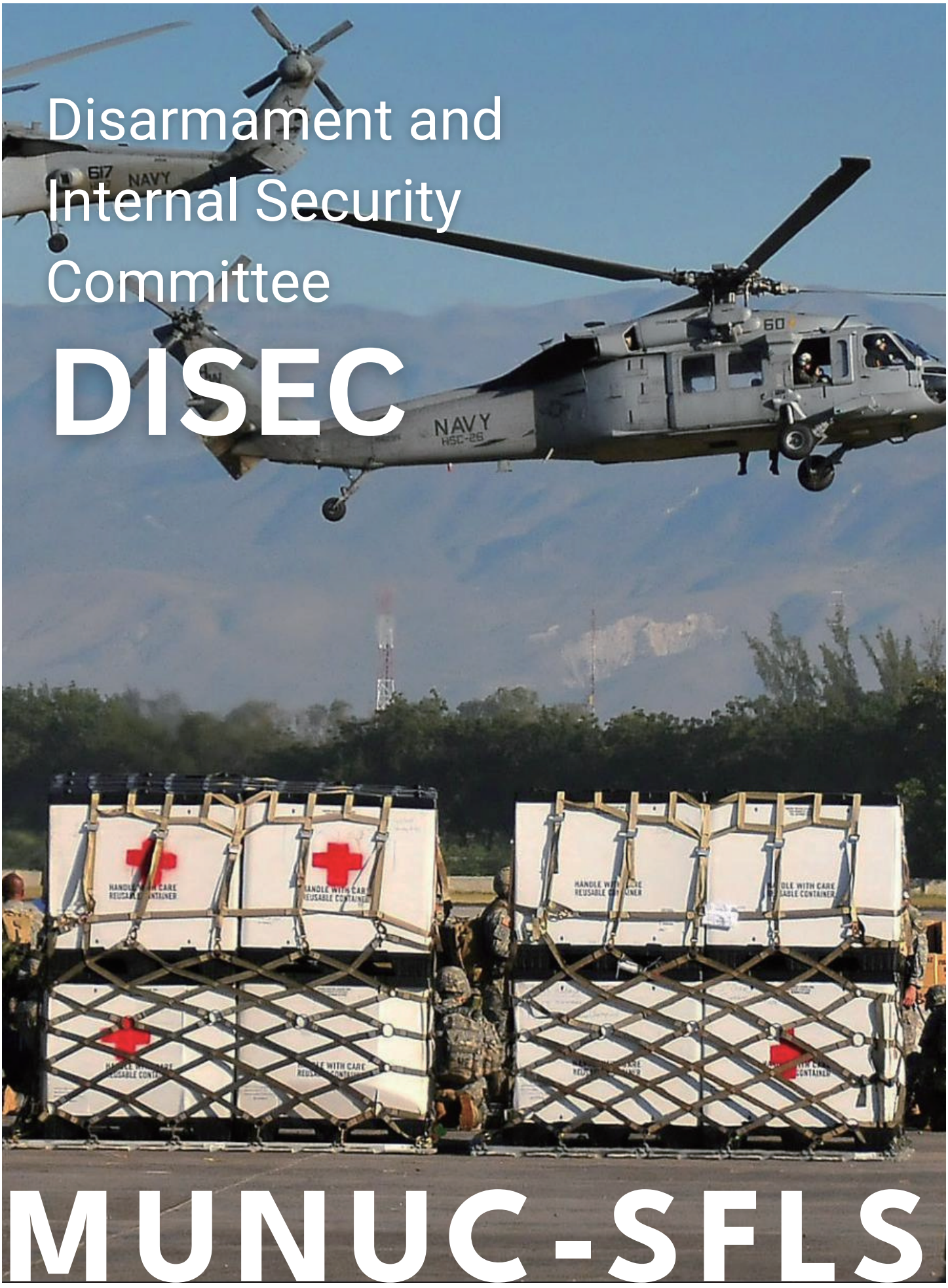
MUNUC-SFLS

Conference

上海外国语大学附属外国语学校
芝加哥大学国际模拟联合国大会

Disarmament and International Security Committee (DISEC)





Disarmament and Internal Security Committee

DISEC

MUNUC-SFLS

Model United Nations of the University of Chicago

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.

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.[7] 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.

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

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

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.

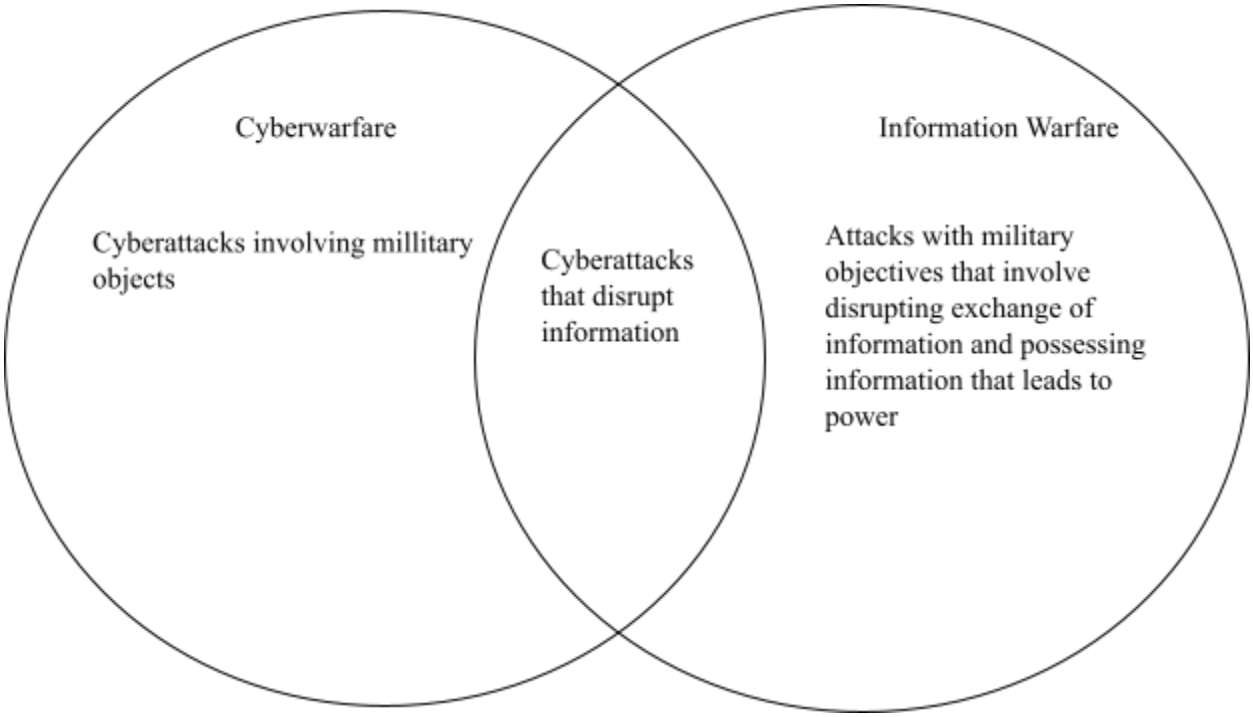
John Sandage, former Director of the Division for Treaty Affairs at the United Nations Office on Drugs and Crime, speaks during a panel on cybersecurity and cybercrime.[8]

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.

[8] "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.[9] 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

[9] 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,[10] 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.[11] 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.[12] 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.[13] 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

---

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

[11] 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.

[12] 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

[13] "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.[14] 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.[15]

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.[16] 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

---

[14] 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.

[15] Ibid.

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

and 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,[17] 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.

[17] 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.[18]

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.[19] 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

---

[18] "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.

[19] 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.

assault on a state",[20] referring to the use of cyberspace to conduct military attacks. These attacks limited Estonians' access to their money, disrupted communication between government officials as well as civilians, and exposed the possibility for cyberattacks to cause long-lasting damage.[21] 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.[22] 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,[23] 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.**[24] 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.[25]

---

[20] 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.

[21] "2007 Cyber Attacks on Estonia," NATO Strategic Communications Centre of Excellence, n.d., https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf.

[22] Ibid.

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

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

[25] Ibid.

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 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.[26] 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.[27] During the war, Georgian government websites were shut down by hackers,[28] 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.[29] It's important to also note that the Russian news agency RIA Novosti was also targeted by a cyberattack.

---

[26] 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.

[27] 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.

[28] 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.

[29] 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/.

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 succeeded in its ability to reach the West by always maintaining media access to English speaking ministers,[30] 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.[31] 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,[32] 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

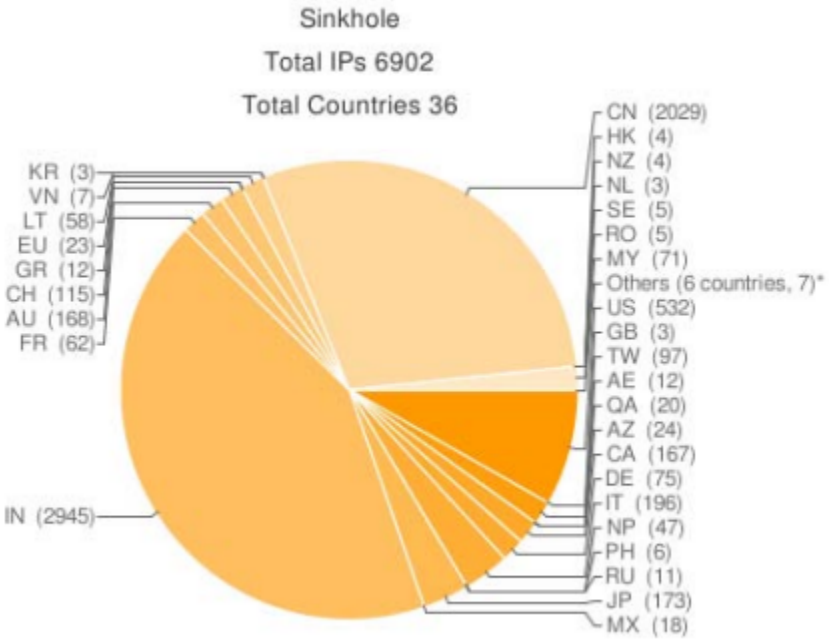
---

[30] 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.

[31] 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.

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

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. 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.[33]

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

[33] 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.[34]

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.[35] Following these events, Iranian news sources reported that a malware was affecting many industries across Iran, but not recognizing specific sites.[36] 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.[37] Delegates should use this cyber incident to consider how incidents of cyberwarfare can have far-reaching effects beyond just the cyberspace.

---

[34] 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.

[35] Ibid.

[36] 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.

[37] 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.[38]

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.[39] They also noted that there were no findings suggesting that votes themselves were changed or manipulated, but they did find that the information of these voters was vulnerable and was stolen. The damages of the incident are

---

[38] 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.

[39] "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.

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.[40] 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.

---

[40] 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.[41] 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",[42] 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.[43] 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

---

[41] "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.

[42] "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.

[43] 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.[44] Most importantly, the resolution established a "group of governmental experts ... to study existing and potential threats in the sphere of information security."[45] 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.[46]

The reports clarify that states should not knowingly allow their territory to be used for "internationally wrongful acts using [information & communication technology]",[47] 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

---

[44] Ibid.

[45] "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.

[46] "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.

[47] "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.[48]

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.[49]

[48] "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.

[49] 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.[50] 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.[51] 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.[52] 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.

---

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

[51] "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.

[52] "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.[53]

[53] 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/.