PREPMUN 2019

DISARMAMENT & INTERNATIONAL SECURITY COMMITTEE STUDY GUIDE

WELCOME LETTER FROM THE DAIS

Dear Delegates,

From the dais of DISEC, welcome to PREPMUN 2019! We are very pleased to be chairing this council and we hope you all will have an enjoyable and enriching time here. Whilst the topics may seem daunting and the council may appear foreign, rest assured that we as your dais will guide you through these 4 days of council debate. However, be prepared. Although we will guide you, we will push you to become better versions of yourselves than you were before.

As its name suggests, DISEC, also known as the Disarmament and International Security Committee, is charged with the duty of handling topics related to disarmament and international security on the UN Agenda. While the topics it handles are similar to the Security Council, make no mistake that DISEC is at its core a General Assembly Committee. As such, it is unable to produce legally binding resolutions, but can make recommendations for further action to the General Assembly itself.

Regardless of whether or not you've had a background in public speaking or you're taking your first steps into the circuit, we as the dais of DISEC promise to give our very best in this committee and only ask that you do the same as well. If you need to contact us, feel free to drop us an email at disec.prepmun@gmail.com.

With that, we all look forward to seeing you at PREPMUN soon!

Yours sincerely,
Bernard Lau, Ee Ying Qi and Lubna Shah
Dais of the Disarmament and International Security Committee

DAIS INTRODUCTION

Bernard Lau - Head Chair

There are only 3 things that Bernard can derive joy from in his short lifespan on earth as of now: MUN, a Konigstiger's destructive elegance, and Crisis councils. Having spent his secondary 2 and 3 life dedicated entirely to MUN and all the work that comes with it, it's safe for him to say that he's just about ready to go on hiatus and prepare for his O levels. In between deadlines for anything and everything, gaming sessions along with moments of respite and tea fill the gaps before his phone blows up with work. He hopes that all delegates will have a fun and fruitful experience at PREPMUN 2019.

Ee Ying Qi - Deputy Chair

Ying Qi unexpectedly found herself in the MUN circuit, something she would never have voluntarily joined, if not for the desperate pleas of a friend who could not attend at the last minute. Being a first-timer allocated to a crisis council was both daunting and, oftentimes, disconcerting, but at the end of the day she found herself more confident, and more interested in current affairs. Ever since, MUN has been an integral part of her life, providing a welcoming respite from the reality of schoolwork and CCA. Ying Qi wishes that all delegates would similarly find their places in the MUN circuit and most importantly, have an enjoyable and fulfilling time at DISEC.

Lubna Shah - Deputy Chair

Lubna is a Year 2 student at Raffles Girls' School. Due to her young age, she has to contend with being the shortest of her council. However, despite being vertically challenged, Lubna is very pleased that at the time of writing, she has delled at 4 conferences and is going to chair at PREPMUN. Outside of MUN, she plays chess competitively and enjoys science research. She is excited to meet all delegates and hopes they will enjoy themselves at the conference.

INTRODUCTION TO THE COMMITTEE

Disarmament and International Security Committee (DISEC)

When the UN was first established, the General Assembly became the principal organ in ensuring the proper functioning of the UN. The General Assembly was split into 6 different committees, each specialising in different topics on the UN Agenda. The First Committee, now known as the Disarmament and International Security Council (DISEC), was dedicated to discussing topics of Disarmament and International Security.[1]

As one of the main 6 committees, DISEC serves as an advisory body to the General Assembly and produces recommended solutions and Resolutions to be voted on.[2] As such, similar to the General Assembly, none of its resolutions are legally binding in any effect.

DISEC seeks to improve international security and deals with issues pertaining to weapons and disarmament. However, documents covered by DISEC mainly involve minor amendments to existing documents and resolutions.[3]

[1] "United Nations General Assembly". 2019. Encyclopedia Britannica. https://www.britannica.com/topic/United-Nations-General-Assembly.
[2] "United Nations First Committee | Treaties & Regimes | NTI". 2019. Nti.Org. https://www.nti.org/learn/treaties-and-regimes/un-first-committee/.
[3] Ibid.

TOPIC A: QUESTION OF REGULATING AND DISARMING CHEMICAL WEAPONS

Introduction to the Topic

The first usage of modern chemical weapons dates back to 1916. During World War 1, chlorine gas was released at the town of Ypres, causing fear and panic. 9 years later the 1925 Geneva Convention would ban them from being used in warfare. However, it had failed to prevent their usage during World War 2, especially with Zyklon B during the Holocaust.

Since World War 2, the world has come a long way in introducing regulations against chemical weapons. The most monumental among them being the Chemical Weapons Convention, which as of 2019 has been recognized by 193 member states.

However, there are still flaws and loopholes in these regulations. In 2018, the Douma attack shocked the whole world with its brutality, the usage of chemical weapons against civilians. Adding on to this, many companies have been implicated in the sale of chemical components to Syria, with said components being essential to the production of chemical weapons.

Background Information

Historical Developments

The first modern attempts at regulating chemical weapons appeared in the Brussels Declaration of 1874, whereby under Article 13(a) 'Employment of poison or poisoned weapons was forbidden.'[4] 25 years later, the 1899 Hague convention would reinforce this under Article 23,[5] and again, later in the 1907 Hague convention under Article 23 with the exact same wording.[6] Despite these attempts, the usage of chemical weapons during World War 1 would reveal their flaws when put into practical effect. This resulted in public uproar over the brutality of chemical weapons, leading to further restrictions being introduced in the 1925 Geneva Convention. Under the convention, although usage of chemical weapons in warfare was banned, production and distribution was still allowed. World War II would expose the flaws of these new regulations. During the War, Zyklon B, originally an industrial pesticide, was used as a means of killing those sent to concentration camps. Thus, when the war ended, there was a greater call for the regulation of chemical weapons to prevent a repeat of history.

[4] Brussels Declaration 1874. Accessed August 19, 2019. https://web.ics.purdue.edu/~wggray/Teaching/His300/Handouts/Brussels-1874.html.
[5] "Convention (II) with Respect to the Laws and Customs of War on Land and Its Annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 29 July 1899." Accessed August 20, 2019. http://www.opbw.org/int_inst/sec_docs/1899HC-TEXT.pdf.
[6] "Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907." Accessed August 20, 2019. http://www.opbw.org/int_inst/sec_docs/1907HC-TEXT.pdf.

Recent Developments

The most monumental development in the area of regulations comes from the Chemical Weapons Convention (CWC) signed in 1997, as it was backed by international law and legally binding to all signatories. Regulations on production and proliferation along with proper procedures for disposal were also introduced. As it stands, the CWC is the most effective measure yet. Nations which had possessed chemical weapons had also declared their commitment to disarming and disposing of these weapons. As of 2019, the United States and Russia remains as the world's last known holders of chemical weapon stockpiles, though the former plans to complete disarmament by 2023[7] and the latter by 2020.[8] However, some states still possess and even use chemical weapons. The Douma chemical attack in 2018 is a clear indicator that the Assad regime continues to own chemical weapons without declaration despite a clear ban on possessing them as outlined by their commitment to the Chemical Weapons Convention. As such, more regulation is required to ensure that states have no undeclared chemical weapons stockpile to enforce present treaties.

In addition, there is controversy over corporations selling chemicals crucial to creating chemical weapons to terrorist organisations or other states. For example, Brenntag, a major German chemical company was suspected of selling dual use chemicals to Syria. Said chemicals were suspected to be used in the Douma attacks.[9] However, the sale of chemical components by private entities remains unaddressed by any international agreement.

The Douma attack alone already highlights the need to regulate and disarm chemical weapons for both state and non-state entities. Although there are far fewer nations that currently possess chemical weapons, rogue states such as Syria continue to use them without fear of consequences.

Key Definitions

Chemical Weapon: A chemical weapon is defined by the Organisation for the Prohibition of Chemical Weapons (OPCW) as "a chemical used to cause intentional death or harm through its toxic properties".[10]

Dual Use Chemicals: A chemical that is defined by the OPCW as "chemicals or equipment that can be used for peaceful civilian and commercial purposes, but can also be used in the creation of weapons or as weapons."[11]

[7] "United States." Nuclear Threat Initiative - Ten Years of Building a Safer World. Accessed August 16, 2019. https://www.nti.org/learn/countries/united-states/chemical/.
[8] "Russia." Nuclear Threat Initiative - Ten Years of Building a Safer World. Accessed August 16, 2019. https://www.nti.org/learn/countries/united-states/chemical/.
[9] "Germany Should Investigate Chemical Weapons-Related Sales to Syria." The Jerusalem Post | JPost.com, August 23, 2019. https://www.jpost.com/Middle-East/Germany-should-investigate-chemical-weapons-related-sales-to-Syria-599436.
[10] "What Is a Chemical Weapon?" OPCW. Accessed August 20, 2019. https://www.opcw.org/our-work/what-chemical-weapon.
[11] Ibid.

Key Issues

Failing Regulations on State Actors

A key aspect in the management and removal of chemical weapons as a weapon of war has been the numerous regulations introduced to keep nations in check. At first these regulations banned their usage in war, without any provisions for production or storage of chemical weapons. However, with the introduction of the CWC, the production and storage of chemical weapons was banned, and existing stockpiles were to be destroyed.

Whilst this marked the end of chemical weapons, this peace would be short lived. With the Douma attack and the Novichok attacks, it was clear that the regulations were faltering and beginning to show its failures. Although the Chemical Weapons Convention was comprehensive, it could not be used to invest authority to disarm a nation of their chemical weapons. This flaw allowed for Syria to develop their own chemical weapons program, while it is suspected that Russia is also beginning to continue development.

The Issue of Dual Use Chemicals

Dual use chemicals are chemicals that can be used for peaceful purposes or as weapons, as defined by the OPCW. Although regulations have been introduced to limit their usage as they can easily be used as chemical weapons under the guise of commercial products. As such, they still remain an issue that has to be addressed in full.

Currently existing regulations have placed restrictions rather than total bans on dual use chemicals, as they still possess a commercial use. However, these chemicals are still used as chemical weapons in spite of existing measures. For example, it was believed that they were used as part of the Syrian Douma attack.

Scope of Debate

Types of Chemical Weapons

Chemical weapons are classified into seven types: choking agents, blister agents, blood agents, incapacitating agents, cytotoxic proteins, nerve agents and lachrymatory agents.[1] Herbicides such as Agent Orange are also considered chemical weapons. The three more contentious types will be covered: herbicides, nerve agents and lachrymatory agents.

Herbicides[12]
Herbicides are chemicals designed to kill unwanted plants in fields such as weeds and invasive species. These herbicides gained more popularity in the 1940s. In battle, their intended purpose is to destroy natural cover and crops that the enemy can leverage on they cause persistent health effects such as genetic disorders, as seen in the Vietnam war.[13] Herbicides

[12] "Convention of the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction." Organisation for the Prohibition of Chemical Weapons. Accessed August 3, 2019. https://www.opcw.org/sites/default/files/documents/CWC/CWC_en.pdf
[13] Fisher, Nicole. "The Shocking Health Effects Of Agent Orange Now A Legacy Of Military Death." Forbes. May 30, 2019. Accessed August 7, 2019.

are banned from being used as a weapon under the CWC, due to the death and harm they can cause.

Nerve Agents
Nerve agents are chemicals weapons designed against the human nervous system. These agents are deadly, as they devastate the human body by shutting down the nervous system. Under the Chemical Weapons Convention, they are covered under the blanket ban on chemical weapons in Article 1.

Riot Control Agents
Riot control agents which are used in protests to disperse violent crowds and subdue violent individuals. The use of riot control agents in warfare is prohibited by the CWC.[14] However, they are permitted for use in "law enforcement, including domestic riot control purposes". However, a study of reports from the UN, regional human rights bodies and international NGOs identified human rights violations committed by law enforcement agents using riot control agents in at least 95 countries or territories from 2009 to 2013.[15] Yet, there are nations that have signed the CWC remaining silent on this issue. OPCW has not clarified either regarding the definition and extent of "law enforcement".

Regulations on States Regarding the Stockpiling and Use of Chemical Weapons

The immorality of the use of chemical weapons has been codified in international norms such as the International Humanitarian Law and *jus in bello* principles,[16] which recognise these weapons as "agents of unnecessary suffering".

Yet, it may be unreasonable to regulate chemical weapons as it may violate state sovereignty. The 1648 Treaty of Westphalia recognises state sovereignty as the foundation of international relations, which grant states complete monopoly over internal affairs, including the possession of chemical weapons.

In response to a need for intervention in nations to prevent genocides, the 2005 Responsibility to Protect (R2P) initiative was passed consensually to resolve conflicting ideals of international norms - the international community's obligation to protect human rights and state sovereignty. The R2P allows the United Nations to assist states in preventing the listed crimes and in particular, allows the OPCW to facilitate disarmament of chemical weapons through the CWC with little opposition.[17]

---

https://www.forbes.com/sites/nicolefisher/2018/05/28/the-shocking-health-effects-of-agent-orange-now-a-legacy-of-military-death/#387bc96621c6.
[14] "Convention of the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction." Organisation for the Prohibition of Chemical Weapons. Accessed August 3, 2019. https://www.opcw.org/sites/default/files/documents/CWC/CWC_en.pdf
[15] Crowley, Micheal. "Arms Control Today." Perilous Paths: Weaponizing Toxic Chemicals for Law Enforcement | Arms Control Association. Arms Control Association , March 2016. https://www.armscontrol.org/act/2016-03/features/perilous-paths weaponizing-toxic-chemicals-law-enforcement.
[16] Zanders, Jean Pascal. "International Norms against Chemical and Biological Warfare: An Ambiguous Legacy." *Journal of Conflict & Security Law* 8, no. 2 (2003): 391-410. http://www.jstor.org/stable/26294282.
[17] Gartner, Scott Sigmund. "Obliterating Chemical Weapons Eliminates Both a Silent Killer and a Threat to the Concept of Exclusive State Sovereignty." HuffPost. November 27, 2013. Accessed August 18, 2019. https://www.huffpost.com/entry/obliterating-chemical-wea_b_4002121.

Although the OPCW has been successful in achieving the large-scale destruction of chemical weapons, key issues remain regarding conflicting international norms that impede the complete destruction of such weapons.

Balance between protection of state sovereignty and respect of human rights is asymmetrical; it is largely attributed to the level of international influence of respective states, effectively undermining the legitimacy of the R2P and similar international norms. For small states with little political and economic influence, coercion into compliance with such international human rights norms, typically through the combined influence of the international community or a major superpower, can easily be achieved. Yet, gross violations by significantly larger states or even permanent members of the United Nations Security Council remain unchecked, due to insufficient political influence or willpower by other states.[18] Furthermore, the enforcement of international norms, mainly influenced by superpowers, are largely aligned with national interests. This means that there is a double standard applied to certain nations. For example, Russia had completely disregarded the Novichok attack despite overwhelming evidence that pointed to Russia being the perpetrators of the incident. As such, powerful nations continue to receive so-called "immunity" despite the fact that all states, irrespective of status, should be held equally accountable for any wrongdoing.

Such an issue manifests itself acutely during the Syrian Civil War. The Assad regime is still unaccountable for the usage of chemical weapons, most recently the 2017 Khan Shaykhun chemical attack and the 2018 Douma chemical attack. While these attacks resulted in international condemnation and incited military action from the US, Britain and France, the Assad regime faced little legal consequences which curb the perpetuation of such atrocities. In fact, Russia and China's continuous support of the regime and their condemnation of the US's military action in defense of Syria's state sovereignty shields Assad so that his regime can continue the use of chemical weapons.[19]

Oftentimes, the selective application of international norms and principles are merely justifications for large states acting on national interests. Even as the Assad regime deserves legal and international implications, intervention may not be the best way to deal with the situation. Intervention might be counterproductive, as it might actually make the situation there worse. As such, agreements on clear guidelines to enforce[20] demilitarisation of chemical weapons that can be applied universally is needed.

Regulations on Non-State Actors

Currently, concerns regarding the development, acquisition and use of chemical weapons by private individuals or terrorist organisations are growing. Those that seek to acquire weapons may be states attempting to get around regulations. Non-state actors in this scenario mainly covers private entities such as companies, as these organisations are capable of legally and

[18] Menon, Rajan. "The Fatal Flaws of R2P." Atlantic Council. Accessed August 19, 2019. https://www.atlanticcouncil.org/blogs/new-atlanticist/the-fatal-flaws-of-r2p.
[19] Naik, Ameya Ashok, Aykan Erdemir, Adam Lupel, Alex J. Bellamy, Alice Debarre, Benjamin Duerr, Francesco Mancini, and Jose Vericat. "Syria and the Crisis of Sovereignty." IPI Global Observatory. April 07, 2017. Accessed August 12, 2019. https://theglobalobservatory.org/2017/04/syria-assad-chemical-weapons-idlib-sovereignty/.
[20] "Confrontation at the OPCW: How Will the International Community Handle Syria and Skripal?" War on the Rocks. June 18, 2018. Accessed August 19, 2019. https://warontherocks.com/2018/06/confrontation-at-the-opcw-how-will-the-international-community-handle-syria-and-skripal/.

reasonably producing the needed components for chemical weapons or procuring such chemicals for usage as chemical weapons if they intend to. An example would be how the Japanese cult Aum Shinrikyo had staged the infamous 1995 Tokyo attacks with Sarin gas. The gas had been acquired via companies owned by the cult.[21]

In terms of producing chemical weapons, non-state actors are an essential supply partner for countries that continue to maintain a stockpile of them. Commercial chemicals are also used in the manufacture of chemical weapons. For example, chemicals used for pharmaceutical drugs are also used in the production of VX and Sarin Gas, both of which are chemical weapons.[22] Hence, countries legally purchase chemicals used in commercial production to develop their on chemical weapons from non-state actors. To address this, regional organisations and nations have implemented regulations on these chemicals. A national example would be Singapore. In Singapore, controlled chemicals which can be used as weapons such as Sarin are regulated and require a license to import. Failure to comply with the licensing requirements would result in a fine, jail time or both. Regionally, the European Union has implemented the Prior Informed Consent Regulation, which placed total bans and heavy restrictions on what they call 'hazardous chemicals'. However the punishment for offenders is left to the discretion of individual nations.[23]

As such, delegates must consider what exactly would warrant punishment in terms of what chemical components companies can or cannot produce and limitations on export of said chemicals.

Although many treaties which facilitate the management of chemical weapons exist, such as the Bilateral Disarmament Agreement between the United States and Russia to destroy existing chemical stockpiles,[24] delegates should also look into introducing further measures to limit chemical weapons and their usage by states or other entities. Such measures may encompass prevention of non-state actors (e.g. terrorists) from using and acquiring chemical weapons, disposal of chemical weapons with the intent of increasing global security, and place further limits on whether or not states are allowed to possess or use chemical weapons in any capacity, and incentivising states to adhere to existing conventions. Such conventions mainly include the Chemical Weapons Convention.

For example, in 2018, 3 Belgian companies came under investigation by Belgian prosecutors selling chemicals required to make Sarin Gas, a nerve agent, to Syria.[25] This highlights the further need to impose regulations on companies to prevent further sale and proliferation of

[21] Walters, Ho Douglas B., Pauline, Hardesty, and Jasper. "Safety, Security and Dual-use Chemicals." Journal of Chemical Health and Safety. December 18, 2014. Accessed August 18, 2019. https://www.osti.gov/pages/servlets/purl/1340249.
[22] Deutsche Welle. "German Firms Sent Weapons-grade Chemicals to Syria despite Sanctions - Report: DW: 25.06.2019." DW.COM. Accessed August 15, 2019. https://www.dw.com/en/german-firms-sent-weapons-grade-chemicals-to-syria-despite-sanctions-report/a-49355063.
[23] "PIC Legislation." ECHA. European Chemicals Agency, n.d. https://echa.europa.eu/regulations/prior-informed-consent/legislation.
[24] "Summit in Washington Summary of U.S.-Soviet Agreement on Chemical Arms." The New York Times. June 02, 1990. Accessed August 19, 2019. https://www.nytimes.com/1990/06/02/world/summit-in-washington-summary-of-us-soviet-agreement-on-chemical-arms.html.
[25] Boffey, Daniel. "Belgian Firms Prosecuted over Syria Chemical Exports." The Guardian. April 18, 2018. Accessed August 15, 2019. https://www.theguardian.com/world/2018/apr/18/belgian-firms-prosecuted-over-chemicals-exports-to-syria-sarin.

chemical weapons. These regulations may include placing restrictions on the sale of any commercial chemicals that can be used in the production of chemical weapons as previously implemented by the EU.[26] At the same time it is essential to ensure that regulation is not too excessive, as these chemicals, despite their usage in weapons are still essential commercial goods.

Therefore, it is important to ensure a balance between corporate interest of profit-making and advancing research, along with the international interests of ensuring proper regulations and preventing the use of chemical weapons in war.

Preventing Commercial Chemicals from Becoming Chemical Weapons

Many commercial chemicals have been utilised as chemical weapons before, one example being the development of a pesticide in Germany called Tabun in 1938. This would later become known as Sarin gas, a deadlier variant of Tabun. In more modern day situations, toxic gases such as chlorine and cyanides are more commonly used for pharmaceutical and production purposes.[27] These chemicals are known as dual use chemicals; chemicals which can be used for beneficial or harmful purposes.[28]

At an international level with increased trade between countries, dual use chemicals may inadvertently slip by under the guise of being commercial goods. For example, British companies were given permits to sell chemicals to Syria between 2004 and 2010. However, they were revoked after it was found that said chemicals could be turned into chemical weapons.[29] Despite attempts to stop the sale, these chemicals would later be confirmed to have been involved in creating the chemicals used in the Damascus attack.[30] Therefore, in order to prevent commercial chemicals from being used as chemical weapons, it is essential to prevent dual use or restricted chemicals from being traded into the wrong hands.

Another issue is that corrupt individuals will sell chemicals for the purposes of creating chemical weapons to states.[31] For example, Frans Cornelis Adrianus van Anraat, a Dutchman, was found guilty of war crimes for purchasing chemicals from America and Japan in order to sell it to Syria for them to produce chemical weapons.[32] This further highlights the need to prevent the misappropriation of dual use chemicals as chemical weapons.

[26] "List of Chemicals: Annex I." ECHA. Accessed August 19, 2019. https://echa.europa.eu/regulations/prior-informed-consent/list-chemicals.
[27] Ganesan, K., S. K. Raza, and R. Vijayaraghavan. "Chemical Warfare Agents." Journal of Pharmacy & Bioallied Sciences. July 2010. Accessed August 14, 2019. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3148621/.
[28] Walters, Douglas B., Ho, Pauline, and Hardesty, Jasper. Thu . "Safety, security and dual-use chemicals". United States. doi:10.1016/j.jchas.2014.12.001. https://www.osti.gov/servlets/purl/1340249.
[29] Norton-Taylor, Richard. "UK Approved More Chemical Exports to Syria than Previously Revealed." The Guardian. September 11, 2013. Accessed August 15, 2019. https://www.theguardian.com/world/2013/sep/11/uk-officials-chemical-exports-syria.
[30] Hopkins, Nick. "Syrian Conflict: Key Sarin Ingredients Sold by UK Firms." BBC News. July 09, 2014. Accessed August 15, 2019. https://www.bbc.com/news/uk-28212724.
[31] "The Future of Chemical Weapons." The New Atlantis. Accessed August 8, 2019. https://www.thenewatlantis.com/publications/the-future-of-chemical-weapons.
[32] "Public Prosecutor v. Frans Cornelis Adrianus Van Anraat." ICD - Van Anraat - Asser Institute. Accessed August 17, 2019. http://www.internationalcrimesdatabase.org/Case/178/Van-Anraat/.

Currently, the main methods of preventing this is via national regulations and bans. For example, the European Union currently has a list of dual use chemicals that are restricted for trade, although companies can be permitted to trade by competent authorities.[33]

Shortcomings of the Chemical Weapons Convention

Although the Chemical Weapons Convention has received near global recognition, there are still certain areas in which it sometimes falls shorts. This mainly comes in the OPCW and how it currently functions.

Taking the Douma attacks as an example, the effectiveness of the OPCW had been called into severe question after their investigations. In the aftermath of the attack, the OPCW was blocked from entering the area by the Russians and Syrians who had occupied the area. This raised suspicions that there was a sort of 'clean up' going on, with crucial evidence potentially being erased.[34]

Rather than any concerted action, the OPCW split in two. One blamed the Western bloc for staging the attacks,[35] the other at Syria for conducting these attacks.[36] This highlights the weakness of the OPCW in affirmatively resolving such disputes, as their mandate is limited to only confirming the presence of chemical weapons. Hence, they are not empowered to accuse nations of deploying said weapons.

To prevent further erosion of the mandate of the CWC and OPCW, the following question has to be asked: how can the CWC and its mandate be expanded to further improve effectiveness and cover a wider scope?

Potential Solutions

Introducing Limitations on the Export Ability of Non-State Actors

Although nations currently have restrictions placed on their ability to proliferate chemical weapons via limitations on chemicals they can purchase for these purposes, there have been no universal restrictions on non-state actors and their ability to sell these chemicals to states. This inevitably leads to a situation where companies may begin selling chemical components to states for the purpose of producing chemical weapons under the guise of commercial trade. There may be another situation where companies may start selling chemical components for these weapons to terrorist organisations or individuals with unknown intent and motivations.

On an international level, another possible solution would be the introduction of a universal restriction on dangerous chemicals used in the creation of chemical weapons. Although this

[33] "European Commission Directorate-General for Trade." Dual-use Trade Controls - Trade - European Commission. Accessed August 19, 2019. https://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/.
[34] Pérez-peña, Richard, and Rick Gladstone. "Chemical Arms Experts Blocked From Site of Syria Attack." The New York Times. April 16, 2018. Accessed August 18, 2019. https://www.nytimes.com/2018/04/16/world/middleeast/syria-douma-chemical-attack.html.
[35] Wintour, Patrick. "'Obscene Masquerade': Russia Criticised over Douma Chemical Attack Denial." The Guardian. April 26, 2018. Accessed August 13, 2019. https://www.theguardian.com/world/2018/apr/26/obscene-masquerade-russia-criticised-over-douma-chemical-attack-denial.
[36] "US Hails OPCW Report on Douma, Syria Chlorine Attack." Middle East Monitor. March 07, 2019. Accessed August 15, 2019. https://www.middleeastmonitor.com/20190307-us-hails-opcw-report-on-douma-syria-chlorine-attack/.

would allow for the supply of chemicals for chemical weapons to run dry and effectively prevent production, this does have implications for other industries, as many chemicals they require are used in chemical weapons.

Introducing Further Restrictions on the Trade of Dual Use Chemicals

Although restrictions and regulations on the trade of dual use chemicals do exist, there have been occasions where these have failed such as in the case of British firms trading them to Syria. As such, another solution would be to introduce further restrictions on the trade of dual use chemicals. For example, as most countries exporting these chemicals are the ones granting permits, countries importing them should also be given the power to a certain degree to seize them. The idea being that if the countries sees it as a threat, it would be empowered to seize the chemicals and conduct necessary investigations.

Guiding Questions

1. What would be the consequences of placing absolute regulations on companies involved in the chemical industry?

2. How can we ensure that nations who agree to fully disarm strictly follow regulations introduced?

3. Is the mandate of the Chemical Weapons Convention reaching its limits? If so, can more be done to expand on it?

Questions a Resolution Must Answer (QARMA)

1. How would a resolution ensure the proper disarmament of all hidden and known chemical weapon stockpiles on top of existing agreements?

2. How would a resolution address the involvement of non-state actors, given the murky business and easy concealment?

3. How would a resolution handle the issue of commercial chemicals being weaponized?

4. How would a resolution support existing measures, such as the CWC and regional treaties? Or would it work towards expanding them?

Key Stakeholders

The Syrian Bloc

Syria is thought to possess the world's third-largest stockpile of chemical weapons after United States and Russia. Syria's weapons, which consist of mainly deadly nerve agents that can be delivered by artillery rockets, shells and aircraft munitions, were developed for use against Israel.[37] This shows a clear violation of existing treaties, including the Chemical Weapons Convention (CWC), which Syria is a signatory to. As the Syrian civil war continues, the Syrian government may continue to use chemical weapons while denying accusations of such. It may prove difficult to convince Syria to surrender their chemical weapons, as they may lose a tool to control their population and fight the rebels with.

Nations without chemical weapons

Internationally, under the CWC, most nations have agreed to destroy their remaining chemical weapon stockpiles.

Nations have much to gain from a world free of chemical weapons. For example, the elimination of these attacks will ensure that civilians will not have to suffer the effects of chemical weapons being used against them. This can be seen from the Douma attack, where dozens of civilians in

[37] Warrick, Joby. "Worries Intensify over Syrian Chemical Weapons." The Washington Post. September 06, 2012. Accessed September 27, 2019. https://www.washingtonpost.com/world/national-security/worries-intensify-over-syrian-chemical-weapons/2012/09/06/13889aac-f841-11e1-8253-3f495ae70650_story.html.

the town were killed.[38] Despite this, nations are still unable to legally intervene into another nations sovereign affairs as a solution to remove chemical weapons. Therefore, these nations must instead find alternate means to achieve disarmament of chemical weapons, from regulatory treaties to other means.

Conclusion

Although many nations have agreed to abandon chemical weapons, many nations still actively maintain arsenals. From Russian VX agents to Syria and their chlorine gas, there is still much to be done. Beyond just nations, non-state actors and companies have become important suppliers of chemicals to produce these chemical weapons, some going as far as to use them. With this in mind, delegates should ask the question, how can we create a world without chemical weapons?

[38] Osborne, Samuel. "Syria Civil War: 'Toxic chemical' containing chlorine used in Douma attack, inspectors conclude. The Independent. March 01, 2019. Accessed September 27, 2019. "https://www.independent.co.uk/news/world/middle-east/syria-civil-war-douma-chemical-attack-chlorine-opcw-a8803991.html

Bibliography

1. Boffey, Daniel. "Belgian Firms Prosecuted over Syria Chemical Exports." The Guardian. April 18, 2018. Accessed August 15, 2019. https://www.theguardian.com/world/2018/apr/18/belgian-firms-prosecuted-over-chemicals-exports-to-syria-sarin.
2. Brussels Declaration 1874. Accessed August 19, 2019. https://web.ics.purdue.edu/~wggray/Teaching/His300/Handouts/Brussels-1874.html.
3. "Confrontation at the OPCW: How Will the International Community Handle Syria and Skripal?" War on the Rocks. June 18, 2018. Accessed August 19, 2019. https://warontherocks.com/2018/06/confrontation-at-the-opcw-how-will-the-international-community-handle-syria-and-skripal/.
4. “Convention of the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction.” Organisation for the Prohibition of Chemical Weapons. Accessed August 3, 2019. https://www.opcw.org/sites/default/files/documents/CWC/CWC_en.pdf
5. "Convention (II) with Respect to the Laws and Customs of War on Land and Its Annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 29 July 1899." Accessed August 20, 2019. http://www.opbw.org/int_inst/sec_docs/1899HC-TEXT.pdf.
6. "Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907." Accessed August 20, 2019. http://www.opbw.org/int_inst/sec_docs/1907HC-TEXT.pdf.
7. Crowley, Micheal. “Arms Control Today.” Perilous Paths: Weaponizing Toxic Chemicals for Law Enforcement | Arms Control Association. Arms Control Association , March 2016. https://www.armscontrol.org/act/2016-03/features/perilous-paths weaponizing-toxic-chemicals-law-enforcement.
8. Deutsche Welle. "German Firms Sent Weapons-grade Chemicals to Syria despite Sanctions - Report: DW: 25.06.2019." DW.COM. Accessed August 15, 2019. https://www.dw.com/en/german-firms-sent-weapons-grade-chemicals-to-syria-despite-sanctions-report/a-49355063.
9. "European Commission Directorate-General for Trade." Dual-use Trade Controls - Trade - European Commission. Accessed August 19, 2019. https://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/.
10. Fisher, Nicole. "The Shocking Health Effects Of Agent Orange Now A Legacy Of Military Death." Forbes. May 30, 2019. Accessed August 7, 2019. https://www.forbes.com/sites/nicolefisher/2018/05/28/the-shocking-health-effects-of-agent-orange-now-a-legacy-of-military-death/#387bc96621c6.
11. Ganesan, K., S. K. Raza, and R. Vijayaraghavan. "Chemical Warfare Agents." Journal of Pharmacy & Bioallied Sciences. July 2010. Accessed August 14, 2019. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3148621/.
12. Gartner, Scott Sigmund. "Obliterating Chemical Weapons Eliminates Both a Silent Killer and a Threat to the Concept of Exclusive State Sovereignty." HuffPost. November 27, 2013. Accessed August 18, 2019. https://www.huffpost.com/entry/obliterating-chemical-wea_b_4002121.

13. “Germany Should Investigate Chemical Weapons-Related Sales to Syria.” The Jerusalem Post | JPost.com, August 23, 2019. https://www.jpost.com/Middle-East/Germany-should-investigate-chemical-weapons-related-sales-to-Syria-599436.
14. Hopkins, Nick. "Syrian Conflict: Key Sarin Ingredients Sold by UK Firms." BBC News. July 09, 2014. Accessed August 15, 2019. https://www.bbc.com/news/uk-28212724.
15. "List of Chemicals: Annex I." ECHA. Accessed August 19, 2019. https://echa.europa.eu/regulations/prior-informed-consent/list-chemicals.
16. Menon, Rajan. "The Fatal Flaws of R2P." Atlantic Council. Accessed August 19, 2019. https://www.atlanticcouncil.org/blogs/new-atlanticist/the-fatal-flaws-of-r2p.
17. Naik, Ameya Ashok, Aykan Erdemir, Adam Lupel, Alex J. Bellamy, Alice Debarre, Benjamin Duerr, Francesco Mancini, and Jose Vericat. "Syria and the Crisis of Sovereignty." IPI Global Observatory. April 07, 2017. Accessed August 12, 2019. https://theglobalobservatory.org/2017/04/syria-assad-chemical-weapons-idlib-sovereignty/.
18. Norton-Taylor, Richard. "UK Approved More Chemical Exports to Syria than Previously Revealed." The Guardian. September 11, 2013. Accessed August 15, 2019. https://www.theguardian.com/world/2013/sep/11/uk-officials-chemical-exports-syria.
19. Osborne, Samuel. “Syria Civil War: ‘Toxic chemical’ containing chlorine used in Douma attack, inspectors conclude. The Independent. March 01, 2019. Accessed September 27, 2019. ”https://www.independent.co.uk/news/world/middle-east/syria-civil-war-douma-chemical-attack-chlorine-opcw-a8803991.html
20. Pérez-peña, Richard, and Rick Gladstone. "Chemical Arms Experts Blocked From Site of Syria Attack." The New York Times. April 16, 2018. Accessed August 18, 2019. https://www.nytimes.com/2018/04/16/world/middleeast/syria-douma-chemical-attack.html.
21. "Public Prosecutor v. Frans Cornelis Adrianus Van Anraat." ICD - Van Anraat - Asser Institute. Accessed August 17, 2019. http://www.internationalcrimesdatabase.org/Case/178/Van-Anraat/.
22. “PIC Legislation.” ECHA. European Chemicals Agency, n.d. https://echa.europa.eu/regulations/prior-informed-consent/legislation.
23. "Russia." Nuclear Threat Initiative - Ten Years of Building a Safer World. Accessed August 16, 2019. https://www.nti.org/learn/countries/united-states/chemical/.
24. "Summit in Washington Summary of U.S.-Soviet Agreement on Chemical Arms." The New York Times. June 02, 1990. Accessed August 19, 2019. https://www.nytimes.com/1990/06/02/world/summit-in-washington-summary-of-us-soviet-agreement-on-chemical-arms.html.
25. "The Future of Chemical Weapons." The New Atlantis. Accessed August 8, 2019. https://www.thenewatlantis.com/publications/the-future-of-chemical-weapons.
26. "United Nations First Committee | Treaties & Regimes | NTI". 2019. Nti.Org. https://www.nti.org/learn/treaties-and-regimes/un-first-committee/.
27. "United Nations General Assembly". 2019. Encyclopedia Britannica. https://www.britannica.com/topic/United-Nations-General-Assembly.

28. "United States." Nuclear Threat Initiative - Ten Years of Building a Safer World. Accessed August 16, 2019. https://www.nti.org/learn/countries/united-states/chemical/.
29. "US Hails OPCW Report on Douma, Syria Chlorine Attack." Middle East Monitor. March 07, 2019. Accessed August 15, 2019. https://www.middleeastmonitor.com/20190307-us-hails-opcw-report-on-douma-syria-chlorine-attack/.
30. Walters, Ho Douglas B., Pauline, Hardesty, and Jasper. "Safety, Security and Dual-use Chemicals." Journal of Chemical Health and Safety. December 18, 2014. Accessed August 18, 2019. https://www.osti.gov/pages/servlets/purl/1340249.
31. Warrick, Joby. “Worries Intensify over Syrian Chemical Weapons.” The Washington Post. September 06, 2012. Accessed September 27, 2019. https://www.washingtonpost.com/world/national-security/worries-intensify-over-syrian-chemical-weapons/2012/09/06/13889aac-f841-11e1-8253-3f495ae70650_story.html.
32. "What Is a Chemical Weapon?" OPCW. Accessed August 20, 2019. https://www.opcw.org/our-work/what-chemical-weapon.
33. Wintour, Patrick. "'Obscene Masquerade': Russia Criticised over Douma Chemical Attack Denial." The Guardian. April 26, 2018. Accessed August 13, 2019. https://www.theguardian.com/world/2018/apr/26/obscene-masquerade-russia-criticised-over-douma-chemical-attack-denial.
34. Zanders, Jean Pascal. “International norms against chemical and biological warfare: An ambiguous legacy.” *Journal of Conflict & Security Law* 8, no. 2 (2003): 391-410. http://www.jstor.org/stable/26294282.

TOPIC B: QUESTION OF CYBER WEAPONRY AND CYBER ATTACKS

Introduction to the Topic

As nations begin to modernise and develop in preparation for the future, so too will hackers and malware grow equally as advanced. Since the first attacks in 1988 due to the 'Morris Worm' to modern attacks against Iranian nuclear facilities, attacks have become more advanced and damaging. This poses a new threat, as the latter serves as an important example of how cyber attacks can cripple physical infrastructure.

To address this, many nations have developed their own cyber security solutions. However, globally there has been no consensus on how to handle cyber attacks and their definitions. There has also been no consensus on who to hold responsible for cyber attacks, the individual launching it or the government that sponsors it? Even in addressing this question, a lack of a universal definition makes it difficult to hold governments using their own definition responsible.

As such, nations must be prepared to address these issues: What is a suitable universal definition of a cyber weapon? How will responsibility for an attack be established?

Background Information

Historical Developments

The first most significant cyber attack happened in 1988, when Robert Tappan Morris wrote a computer programme to deduce the number of systems connected to the Internet, but resulted in widespread system errors that were costly to rectify. The programme was dubbed the "Morris Worm", and is the first example of a "distributed denial of service" attack.[39]

In 2014, an elite group of hackers under a wider group known as 'Lazarus' conducted what would have been one of the biggest heists in history by launching a cyberattack on the Bangladesh Bank. The total amount stolen was 100 million dollars, although most of the transactions were blocked and 40 million dollars was recovered.

Subsequently, relentless cyber attacks were conducted by Moscow against Ukraine. From 2015 to 2016, Russian hacking group Sandman launched attacks on electrical companies that resulted in large-scale blackouts and power outages.[40] The subsequent 2017 NotPetya attack propagated and crippled machines worldwide, even though it began from within Ukrainian

[39] Shackelford, Scott, and Indiana University. "What the World's First Cyber Attack Taught Us about Cybersecurity." World Economic Forum. November 5, 2018. Accessed August 20, 2019. https://www.weforum.org/agenda/2018/11/30-years-ago-the-world-s-first-cyberattack-set-the-stage-for-modern-cybersecurity-challenges.

[40] Gilbert, David. "Inside the Massive Cyber War between Russia and Ukraine." Vice. March 29, 2019. Accessed August 20, 2019. https://news.vice.com/en_us/article/bjqe8m/inside-the-massive-cyber-war-between-russia-and-ukraine.

borders.[41] More recently, Russia launched multiple attacks on Ukraine to disrupt and undermine their 2019 elections processes.

Cyber attacks have evolved over the years, becoming more carefully orchestrated and coordinated each time. Especially so for today, they are oftentimes not standalone, but merely one of a series of planned attacks with a clear political agenda. As such, they have become issues of national security due to their increasing scale and geopolitical significance.

Recent Developments

Over the years, cyber attacks have become increasingly difficult and have been carried out using more sophisticated forms of cyber weaponry. As such, there have been measures put in place to curb this growing issue, which are listed below:

UN Group of Governmental Experts (UN GGE)
Since 2004, five groups of governmental experts have been studying the threats posed by the usage of Information and Communication Technology (ICT) systems and the measures to mitigate these threats.[42]

2013 UN GGE Report: Titled "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", the 2013 UN GGE Report highlights the general guidelines states should adhere to in terms of responsible and ethical use of cyberspace, and urges states to tackle domestic inappropriate use of cyber tools. Importantly, countries endorsing the report recognise the applicability of the UN Charter and international law in regulating state use of cyberspace. Additionally, recommendations are made on (i) Confidence-Building Measures and (ii) Capacity-building Measures. Such measures serve to improve state security and enhance their ability to deal with cyber-threats.

2015 UN GGE Report: Pursuant to the 2013 UN GGE report, the 2015 report provides suggestions on how the principles of international law such as state sovereignty and protection of human rights can apply to the use of ICTs, and such guidelines serve as a common understanding among states.

2016 UN GGE Report: The 5th UN GGE was tasked with the objective of understanding how the international law may be applied to the use of ICTs as well as rules governing the responsible behavior of states. However, there was no consensus and as such, no report could be released.[43] Key contentions will be discussed in the following chapters.

One noteworthy effort to resolve legal issues surrounding cyber warfare is the revised Tallinn Cyber-Warfare Manual 2.0, that provides suggestions on how international law may be applied to cyber warfare. The manual serves to provide insight on how key concepts such as sovereignty, due diligence, jurisdiction and law of international responsibility may be applicable

[41] Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Wired. December 07, 2018. Accessed August 20, 2019. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
[42] "Developments in the Field of Information and Telecommunications in the Context of International Security – UNODA." United Nations. Accessed August 20, 2019. https://www.un.org/disarmament/ict-security/.
[43] Grigsby, Alex. "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased." Council on Foreign Relations. November 15, 2018. Accessed August 20, 2019. https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.

to the cyberspace.[44] However, the Tallinn manual remains as an understanding exclusive to NATO states and is almost powerless in regulating cyber security beyond the American alliance.

In addition to regulatory issues, cyber weapons themselves have evolved in complexity, especially with the recent introduction of Artificial Intelligence (AI).[45] Application of AI in cyberattacks render them more successful and destructive. With the AI's remarkable ability to learn and replicate natural behavior, malicious cyber tools are enhanced, and users are more vulnerable to cyber attacks. As such, delegates are encouraged to source for solutions that enable organisations to counter the evolving complexities of cyber weapons in carrying out attacks.

Key Definitions

International Law: International law is the body of legal rules, norms, and standards that apply between sovereign states and other entities that are legally recognised as international actors.[46]

Non-state Actor: A non-state actor is an individual, entity or organisation that possesses a tremendous amount of influence but does not belong or align themselves with a specific country.

[44] "Tallinn Manual 2.0 on the International Law Applicable to Cyber." National Security Archive. April 24, 2019. Accessed August 20, 2019. https://nsarchive.gwu.edu/news/cyber-vault/2019-04-24/tallinn-manual-20-international-law-applicable-cyber-operations.
[45] Dixon, William, and Nicole Eagan. "3 Ways AI Will Change the Nature of Cyber Attacks." World Economic Forum. June 19, 2019. Accessed August 20, 2019. https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/.
[46] Shaw, Malcolm. "International Law." Encyclopædia Britannica. Encyclopædia Britannica, inc., n.d. https://www.britannica.com/topic/international-law.

Key Issues

Lack of a universal definition of cyberweaponry and cyber attacks

Cyber Weapons

The concept of cyber weapons is rather contemporary and is loosely defined as a malware that is developed for military or intelligence purposes. It can be developed for three main objectives - Surveillance/Espionage, Data Theft and Destruction/Sabotage.[47]

At present, there are competing and non-legally binding definitions of cyber weapons. Without a universally-acceptable definition of cyber weapons, states are able to employ the use of offensive cyber tools without being held accountable. They can argue that the "cyber weapons" they are employing have no specific restrictions, and thus, no action can be taken against them. A lack of a universal definition prevents persecution under international courts, as states may use the same argument in justifying their actions.

The "Tallinn Manual on International Law Applicable to Cyber Warfare" defines cyberweapons and cyberweapons systems as 'cyber means of warfare that are by design, use, or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of objects, that is, causing the consequences required for qualification of a cyber operation as an attack'.[48] The Tallinn Manual was commissioned by NATO and written by experts in the field. The manual is one of the most significant developments in establishing a "foundation" for the application of international law to cyber attacks and related incidents.

The United States' Air Force Instruction 51-402 has defined an Air Force cyber capability as "any device or software payload intended to disrupt, deny, degrade, negate, impair or destroy adversarial computer systems, data, activities or capabilities".[49]

The Australian Strategic Policy Institute states that "cyber weapons are cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack.[50] This definition is based on the intent of cyber weapons.

Key differences in existing definitions are (i) characteristics of weapons, and (ii) objectives of the user.[51] It is uncertain whether cyber weapons should be defined by their potential for destruction (eg. dual-use weapons) or if they should take on a narrower definition, one that identifies cyber weapons as cyber-tools with purely destructive capabilities. Additionally, cyber weapons may also be defined by the intent of the user. Hence, while narrower definitions of cyber weapons may exclude other cyber tools which possess devastating offensive capabilities,

[47] Wilson, Clay. "Cyber Weapons: 4 Defining Characteristics." GCN. June 4, 2015. Accessed August 20, 2019. https://gcn.com/articles/2015/06/04/cyber-weapon.aspx.
[48] Wallace, David. "Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis." Accessed August 20, 2019. https://ccdcoe.org/uploads/2018/10/TP-11_2018.pdf.
[49] "Legal Review of Weapons and Cyber Capabilities." July 27, 2011. Accessed August 20, 2019. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-053.pdf.
[50] Tom Uren, Bart Hogeveen and Fergus Harson, "Defining Offensive Cyber Capabilities", *Aspi.Org.Au*, 2018, https://www.aspi.org.au/report/defining-offensive-cyber-capabilities.
[51] Miralis, Dennis. "What Are Cyber Weapons? : Some Competing Definitions." Lexology, September 28, 2018. https://www.lexology.com/library/detail.aspx?g=65179269-c85e-4253-a9a3-5d9ba1c9c906.

broad-based definitions of cyber weapons may compromise cyber tools employed for legitimate purposes such as defence.

Before any agreements can be made, consensus must first be achieved between states on the official definitions and categorisations of cyber weapons in order to prevent exploitation of loopholes and state-centric interpretations of regulations.

Cyber Attacks

Cyber attacks, on the other hand, can be defined by maneuvers intended for offensive purposes against computer based infrastructure. Cyber attacks may fall under two broad-based categories - active attacks and passive attacks. Active attacks are characterised by attempts to alter system resources or affect their operations with the objective of destruction while passive attacks are attempts to make use of information from computer-based systems without affecting system resources.[52]

However, a greater cause of concern is the issue of cyber warfare, a subset of cyber attacks. Cyber warfare refers to cyber attacks that are conducted for strategic or military purposes and often include state involvement.

Firstly, no agreement can be made as to whether information warfare should be categorised under cyber warfare, or if both ideas should be treated as separate entities.[53]

Furthermore, its highly contentious nature can be attributed to the lack of legally-binding and internationally accepted definitions.[54] It is unclear what exactly constitutes a cyber act of war, and if such acts are under the adjudication of existing legal frameworks. For instance, the 1974 UN General Assembly Resolution 3314 outlined the definition of aggression and prohibits interstate aggressive acts. However, while cyber destructive cyber attacks can be considered acts of aggression, the lack of clear language in linking inter-state cyber attacks to aggression and warfare is often exploited by states to conduct attacks through cyber means whilst avoiding accountability.[55] The lack of definition and categorisations of cyber attacks astutely manifests itself in the issues with the applicability of International Law to such attacks, which will be further discussed in the next section.

Accountability of Cyber Attacks

The technological structure of cyberspace like anonymity makes it difficult to trace an attacker's source. Even if a source is identified, it is unclear if the state is responsible for the individual's actions. As such, states using non-state actors and proxies can mask their traces and disassociate themselves from third parties, effectively side-stepping the international legal system.[56]

---

[52] "Active and Passive Attacks in Information Security." GeeksforGeeks, August 9, 2019. https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/.
[53] Aldrich, Richard. "The International Legal Implications of Information Warfare", Airpower Journal Vol. 10, Issue 3 (Fall 1996).
[54] Brownlee, Lisa. "Why 'Cyberwar' Is So Hard To Define." Forbes. Forbes Magazine, July 21, 2015. https://www.forbes.com/sites/lisabrownlee/2015/07/16/why-cyberwar-is-so-hard-to-define/#5572d2d331f1.
[55] Cammack, Chance. "The Stuxnet Worm and Potential Prosecution by the International Criminal Court Under the Newly Defined Crime of Aggression," Tulane Journal of International and Comparative Law, Vol: 20, 2011/01/01.p. 306, 322.
[56] "The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack." Yale Law School, n.d. https://law.yale.edu/sites/default/files/area/center/global/document/2017.05.10_-_law_of_attribution.pdf.

Beyond technical barriers to attribution, it is difficult to hold states accountable. Before any states response (countermeasures, etc.) can be justified, identification and formal attribution to source of attack must be legitimised. States that are victims to these attacks will have to disclose evidence to back their claims that contributes to the legitimacy of these claims. However, states may be unwilling to do so as it would mean disclosure of their intelligence services and technology.

Scope of Debate

Key Contentions in the Applicability of International Law to Cyber Attacks

The international law's applicability to cyberwarfare is ambiguous, which is one of the key failures of the 2016 UN GGE Report. This lack of guidelines affords countries free reign in the cyberspace to conduct cyber operations. For example, Article 3 of the UN Resolution 3314, which lists scenarios that define acts of aggression, led to a general consensus that such acts of aggression are physical in nature, and as such, lack the cyber component that would hold states organising cyber attacks accountable for their actions.

Conflicting viewpoints on the Rights to Self Defence

If International Law is fully applicable to Cyber Warfare, it would mean that states would be allowed self-defence under Article 51 of the UN Charter.[57] Recognising such rights would then require states to define the threshold for 'armed attacks' in cyberspace as stated in the article. With international law in effect, the use of cyberspace (for offensive or retaliatory purposes) will be subjected to scrutiny, which will only permit such employment of force if it can be justified under Article 51. Generally, while international law subjects offending states in the cyberspace to international condemnation, it also justifies retaliation by use of cyberspace.

However, even as self defence in cyberspace may be justified by international law, existing international frameworks are insufficient in permitting all retaliatory measures by states. Many cyber offensive attacks by states may not qualify as 'armed attacks' stipulated in Article 51 due to lack of scale implied by the term even as they can be considered a 'threat or use of force' under Article 2 Chapter 4. Consequently, retaliatory states' actions to these offensives cannot be justified under international law and may result in international backlash. There also exist complexities with permitted state response.[58] A general guideline put forth by Article 51 is the principle of proportionality in deciding the permitted scale of retaliation.[59] However, proportionality of retaliation or defence measures to the actual attack is even harder to be quantified when states employ the use of forces offline in response to cyber offensives. Israeli Defence Forces bombed a building which they claimed housed Hamas hackers, and announced that Israel had successfully defended themselves against cyber attacks.[60] It is still

[57] "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms." Just Security, June 28, 2018. Accessed August 8, 2019. https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.
[58] Karagiannopoulos, Vasileios, and Mark Leiser. "Cyber Attacks Are Rewriting the 'Rules' of Modern Warfare – and We Aren't Prepared for the Consequences." The Conversation, August 6, 2019. Accessed August 28, 2019. http://theconversation.com/cyber-attacks-are-rewriting-the-rules-of-modern-warfare-and-we-arent-prepared-for-the-consequences-117043.
[59] "The Cyber Law of War." The State of Security, January 30, 2018. https://www.tripwire.com/state-of-security/featured/cyber-law-war/.
[60] Newman, Lily Hay. "What Israel's Strike on Hamas Hackers Means For Cyberwar." Wired. Conde Nast, May 6, 2019. Accessed August 28, 2019 https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/.

uncertain if such acts are justified, and additional guidelines for retaliatory measures are thus necessary.

Presently, the allowance of rights to self-defence by affirming the applicability of Article 51 could not be agreed upon due to conflicting national interests. On one hand, Russia may be wary of US retaliation against their systems if a cyber operation is perceived to be a cyber act of war. In contrast, India is rather supportive of such rights as it would affirm a full retaliation against Pakistan's cyber operations. More significantly, countries such as Cuba with inadequate cyber capabilities are hesitant towards reprisals and are fearful of the advantage enjoyed by states with leading cyber capabilities.[61] As such, asymmetries in cyber capabilities contribute significantly towards some states' hesitation towards embracing cyberspace retaliation.

Attribution of cyber attacks

At present, accountability is possible by international law, but there are glaring issues with these laws. Attribution, a constitution of the law of state responsibility, necessitates a close and identifiable link between a state and an act (a cyber attack, in this case). This includes the link between the state and *de facto* or *de jure* organisations, and there must be evidence of empowerment by government authority. Based on International Jurisprudence, there are two criteria governing 'state control'. The first criterion is effective control, which refers to direct state contribution to the act in question. The second criterion is overall control, which is determined by the provision of finance, capacity and instruction. The key issue is that such links are more often than not difficult to be made, and as such, consequences are not warranted on the offending party based on International law, even if such gross violations are evident.

This is manifested acutely in Russia's alleged intervention in the US Presidential elections, where President Vladimir Putin himself directly ordered such a campaign. This act brings to question the attribution standard of instructions. It stipulates that a state can only be held accountable if the instruction is made by the state to be carried out by specific third parties, consequently leading to the incident that violates international law. An arbitrary directive or articulation of a policy is insufficient to constitute evidence for attribution, even if the overall objectives (oftentimes political) between the government and third party actors are aligned. As such, Putin's order for a Russian campaign to intervene in the US Presidential elections does not meet the threshold of 'specific instruction by state' that would hold him accountable for the violation of international law (infringement upon state sovereignty of the US). Additional acts by third parties that are not explicitly ordered by the government will also be attributed only to these private entities, and not the state, even if the state may be the impetus for such actions.

Attribution is especially hard to be determined when delineations of boundaries between state and private actors are increasingly blurred. This is especially so in China, where private entities are largely state-controlled, such as Chinese tech giant Huawei. Malicious acts by private Chinese firms can be attributed to the state if they are *de facto* or there is sufficient state involvement in the firm such as ownership, funding, and managerial control by the state, which is again, hard to be determined. A private firm's support of state policy is also insufficient to hold a state accountable. Hence, it is unclear if malicious acts by private Chinese firms can be

[61] "The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?" Lawfare, July 4, 2017. Accessed August 28, 2019. https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

attributed to the state, seeing as state intervention is evident, but the level of state invention that holds a state responsible for actions of the private entity is hard to be determined.

The simplest way in which attribution can be determined is when the state directly admits to their involvement in any gross act of violation of international law, but such a scenario is highly unlikely.

Issues Regarding Trade and Transfer within the Cyber Weapons Market

Lack of Enforcement Measures

In the cyber weapons market, there is a lack of regulation when it comes to trade and transfer of arms. One of the measures put in place to combat this was the Wassenaar agreement, that has been updated to include potential weapons such as intrusion software. The agreement is consensus-based, and relies on each country's commitment to the agreements laid out. However, there are limited punishments to enforce full compliance to these agreements. Full compliance of participating states is shaky and jeopardised by significant economic benefits from exports of conventional arms, that may override any state's commitment. One of the high-profile cases include France's initial unwillingness to cancel a 1.2 billion euro contract selling helicopters to Russia despite NATO's strong opposition. The contract was ultimately cancelled.[62] With respect to the cyber weapons market, countries may potentially react in a similar manner by breaking traditional stances and violating agreements in favour of highly-profitable cyber weapon trade deals.

Such an issue is further compounded by the lucrative cyber weapons market, with a valuation of USD390 Billion in 2014 and is expected to reach a value of USD521.87 Billion by 2021. Even as states see the benefits of restricting the spread of potentially disastrous technology, they have huge economic incentives to give large tax-paying tech firms the green light to export such vulnerabilities. Furthermore, such firms simply relocate production to other countries without stringent regulations to continue their exports, effectively undermining the agreement. Resultantly, states are increasing tolerant of acts that disregard such an agreement.

Lack of stipulated country of origin

Due to the flexibility of cyberspace, it is extremely difficult to track exports and transfers of cyberweapons, which are often vulnerabilities that can be sent to another party by the click of a button. This is due to the easy anonymity with which illegal traders are able to mask their activities. In addition, transaction of cyber weapons are undocumented due to the virtual nature of interactions between various parties. Firstly, mass collaborations involving multinational parties working on a specific vulnerability calls to question the exact country of origin of such destructive tools as it has to be acknowledged that these tools are a product of multiple stakeholders. Additionally, such products can be stored in clouds, where they are multinational and do not belong to any particular nation. Furthermore, transfer of destructive codes between multinational programmers are known as 'deemed exports', which are legalised, but extremely difficult to be regulated.

[62] Reuters. "France Has 3 Options for Those Mistral Warships It Was Going to Sell to Russia." Business Insider. Business Insider, June 2, 2015. Accessed August 31, 2019. https://www.businessinsider.com/r-sink-or-sell-russia-spat-leaves-france-with-warships-to-spare-2015-6?IR=T.

Regulations on Research and Development

It is generally agreed that curbing research on cyber weapons would negatively affect legitimate cybersecurity research. The value of zero-day vulnerabilities clearly demonstrates this. As codes and operating systems advance in complexity, more flaws in systems will not be detected at first glance by the creators. As such, the finding of zero-day exploits and handing over information on them to developers helps prevent future cyber attacks that could have exploited the vulnerability. On the other hand, research into such a field may fall into the wrong hands of non-state actors, leading to catastrophic cyber attacks. At the same time, this research has also been conducted by nations such as the United States of America which was linked to the WannaCry ransomware attacks.[63]

Additionally, research into cyber tools for offensive purposes are required for R&D to expand defence capabilities and capacities, but little can be done to prevent the exploitation of such tools for cyber attacks. This is the case for the computer virus Brain, which slowed down computers and ate up storage space. Originally, it was intended to be a countermeasure against people pirating software from the creators of Brain[64], who ran a computer shop, but the code was used and converted into malware.[65]

Furthermore, the continued uncertainty of the rules of cyberspace and excessive research into cyber capabilities for both offensive and defensive purposes by any country may result in retaliation from competing nations, potentially escalating into a cyber arms race.

This calls for regulation on areas of research and agreements of cyber weapon research-related norms to resolve the intricacies between research on cyber capabilities for offensive and defensive purposes and prevent the excessive build-up cyber weapons.[66]

Potential Solutions

Arbitration

The use of arbitration can be employed to settle legal issues surrounding cyber attacks, such as attribution, accountability and potential penalties. The victim can report a state-backed cyber attack to an international, independent arbitration body. Arbitrators will make legal judgements based on international laws as well as validity of the claims made by states. Delegates may also choose to draw inspiration from the Dispute Settlement System of the World Trade Organisation. However, arbitration can only be effective if new laws to govern cyberspace are ironed out and agreed upon.

---

[63] "Baltimore Ransomware Attack: NSA Faces Questions." BBC News. BBC, May 27, 2019. Accessed August 31, 2019. https://www.bbc.com/news/technology-48423954.
[64] "Brain -The First Computer Virus Was Created by Two Brothers from Pakistan. They Just Wanted to Prevent Their Customers of Making Illegal Software Copies." The Vintage News, September 7, 2016. https://www.thevintagenews.com/2016/09/08/priority-brain-first-computer-virus-created-two-brothers-pakistan-just-wanted-prevent-customers-making-illegal-software-copies/.
[65] Sharma, Nitin Mohan. "How a Piracy Protection Software Turned into a First Computer Virus." Thrive Global, August 30, 2017. Accessed August 12, 2019. https://thriveglobal.com/stories/how-a-piracy-protection-software-turned-into-a-first-computer-virus/.
[66] Gady, Franz-Stefan. "Trump and Offensive Cyber Warfare." The Diplomat. January 18, 2017. Accessed August 12, 2019. https://thediplomat.com/2017/01/trump-and-offensive-cyber-warfare/

Confidence-building measures
To address the issues of uncontrolled and potentially dangerous proliferation of cyber weapons, confidence building measures for cyber weapons among states can be considered. Such measures aim to increase transparency in research, development, and production of cyber weapons, including the sharing of latest technology among governments to ensure that use and possession of such weapons can be kept in check. This also resolves the issue of possession of dual use and potentially destructive cyber tools for research, capacity building measures, and generally non-malicious purposes.

Countermeasures
Countermeasures can also be considered for state retaliation. These countermeasures are not warranted by the rights to self-defence, as self-defence refer to attacks that result in destruction on the scale of warfare. Countermeasures recognise the damage of cyber attacks even if they have not reached the threshold of cyber warfare, and are meant to allow for state retaliation of these cyber attacks. Such a measure would also serve as a deterrence for states planning cyber attacks such as destruction of network systems.

These suggestions are not meant to limit, but to provide delegates with an idea of potential solutions. Delegates are highly encouraged to expand on these suggestions and explore the various possibilities.

Guiding Questions

1. How will the council reconcile the competing definitions of cyber weapons and cyber attacks, including what constitutes cyber warfare, and prevent the exploitation of loopholes?

2. How can a compromise be made to address differing concerns of states?

3. What are ways in which states can protect themselves from cyber attacks?

4. How can the issue of asymmetric cyber capabilities be addressed?

Questions a Resolution Must Answer (QARMA)

1. How would the resolution define the circumstances in which retaliatory attacks are allowed, and if so, how would the specific criteria be set? In addition, are there instances where different scales of retaliatory attacks are permitted?

2. How would the resolution modify existing international frameworks to allow for states to be held accountable for any malicious cyber attack initiated by the state?

3. How would the resolution regulate dual-use cyber weapons to allow for research and development in areas such as cyber defence while preventing exploitation of such tools for malicious purposes?

4. How would the resolution foster greater cooperation among states to reduce the threat of cyber security?

Key Stakeholders

Members of NATO

The NATO, aligned with US interests, released the Tallinn Manual that serves to regulate cyberspace with reference to international law.[67] US wishes to work on the application of international law on cyber weapons and cyber warfare as opposed to a separate international treaty, with the objective of preserving their freedom to intervene with affairs of other states within the purview of international law.

It must be noted that NATO is a defensive alliance. In other words, NATO will only respond to cyber attacks and refrain from initiating one.

Russia and China

In contrast, China and Russia are pursuant of an international treaty on cyberwarfare and cyber weapons that would preserve their domestic sovereignty and allow them to better manage transnational information. This is based on concerns of transnational flow of data that may spread ideas debilitating to state security and social harmony, as the term 'information security' in Russia is often synonymous with 'cyber security'. They turn instead to the Shanghai Cooperation Organisation (SCO) and the UN International Telecommunications Union (ITU) to discuss such issues. As such, the US is often in disagreement with Russia as they view Russia's approach as a political maneuver to further justify oppressive practices within their regime.[68] North Korea and Iran are largely supportive of such a stance.

Over the years, there has been a global shift towards cyber sovereignty; states such as the United Kingdom and Brazil[69] are increasingly embracing measures that allow state regulation of information flow in cyberspace.

[67] Stevens, Tim. "Cyberweapons: Power and Governance of the invisible". October 2017. Accessed August 28, 2019.
https://www.researchgate.net/publication/320293035_Cyberweapons_power_and_the_governance_of_the_invisible
[68] Arimatsu, Louise. "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations." NATO, n.d. Accessed August 28, 2019.
https://ccdcoe.org/uploads/2012/01/2_3_Arimatsu_ATreatyForGoverningCyber-Weapons.pdf.
[69] "The Global Trend Toward Cyber Sovereignty." Endgame, October 2, 2018. Accessed August 30, 2019.
https://www.endgame.com/blog/technical-blog/global-trend-toward-cyber-sovereignty.

Neutral Bloc

As a manifestation[70] of the competing ideals, two separate resolutions, the Group of Governmental Experts and the Open Ended Working Group (OEWG) were sponsored by the US and Russia respectively in 2018. Little concrete action has yet been taken by both groups, but countries' stances on the issue can be acutely observed from the voting of both resolutions. With some countries voting based on political allegiance, a significant proportion of countries (77, in fact) such as India, Kazakhstan, Indonesia and South Africa voted for both resolutions, attesting to their political neutrality regarding this issue. They generally hold the strong belief that both resolutions can complement each other.[71] Regardless, the general consensus among almost all states is that further regulation of cyberspace, particularly in areas of national security, is needed.

African Union

States in the African Union with comparatively inferior cyber capabilities are looking to build their cyber capabilities to combat malicious cyber attacks.[72] More notably, member states have recently signed the African Union Convention on Cyber Security and Personal Data Protection.[73]

Conclusion

Although many measures and initiatives have been put in place, activities in cyberspace remain largely unchecked. Due to the rapidly advancing technology, it is of paramount importance that such activities are well-regulated. Delegates should consider the various stakeholders - state and non-state actors - in formulating implementable solutions, given all the complex issues with regards to cyber attacks and weapons.

[70] "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased." Council on Foreign Relations. Council on Foreign Relations, n.d. Accessed September 2, 2019. https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.
[71] Tolstukhina, Anastasia. "Two Cyber Resolutions are Better than None." Russian Internal Affairs Council, February 26, 2019. Accessed September 07, 2019. https://russiancouncil.ru/en/analytics-and-comments/analytics/two-cyber-resolutions-are-better-than-none/
[72] Nkusi, Fred K. "AU Galvanises Cyber-Threats into Tougher Cybersecurity." The New Times | Rwanda, July 29, 2018. Accessed August 30, 2019. https://www.newtimes.co.rw/opinions/au-galvanises-cyber-threats-tougher-cybersecurity.
[73] "African Union Convention on Cyber Security and Personal Data Protection." African Union Convention on Cyber Security and Personal Data Protection | African Union, June 3, 2019. Accessed August 30, 2019. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

Bibliography

1. “Active and Passive Attacks in Information Security.” GeeksforGeeks, August 9, 2019. https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/.
2. “African Union Convention on Cyber Security and Personal Data Protection.” African Union Convention on Cyber Security and Personal Data Protection | African Union, June 3, 2019. Accessed August 30, 2019. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.
3. Aldrich, Richard. “The International Legal Implications of Information Warfare”, Airpower Journal Vol. 10, Issue 3 (Fall 1996).
4. Arimatsu, Louise. “A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations.” NATO, n.d. Accessed August 28, 2019. https://ccdcoe.org/uploads/2012/01/2_3_Arimatsu_ATreatyForGoverningCyber-Weapons.pdf.
5. “Baltimore Ransomware Attack: NSA Faces Questions.” BBC News. BBC, May 27, 2019. Accessed August 31, 2019. https://www.bbc.com/news/technology-48423954.
6. “Brain -The First Computer Virus Was Created by Two Brothers from Pakistan. They Just Wanted to Prevent Their Customers of Making Illegal Software Copies.” The Vintage News, September 7, 2016. https://www.thevintagenews.com/2016/09/08/priority-brain-first-computer-virus-created-two-brothers-pakistan-just-wanted-prevent-customers-making-illegal-software-copies/.
7. Brownlee, Lisa. “Why 'Cyberwar' Is So Hard To Define.” Forbes. Forbes Magazine, July 21, 2015. https://www.forbes.com/sites/lisabrownlee/2015/07/16/why-cyberwar-is-so-hard-to-define/#5572d2d331f1.
8. Cammack, Chance. “The Stuxnet Worm and Potential Prosecution by the International Criminal Court Under the Newly Defined Crime of Aggression,” Tulane Journal of International and Comparative Law, Vol: 20, 2011/01/01.p. 306, 322.
9. "Developments in the Field of Information and Telecommunications in the Context of International Security – UNODA." United Nations. Accessed August 20, 2019. https://www.un.org/disarmament/ict-security/.
10. Dixon, William, and Nicole Eagan. "3 Ways AI Will Change the Nature of Cyber Attacks." World Economic Forum. June 19, 2019. Accessed August 20, 2019. https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/.
11. Gady, Franz-Stefan. "Trump and Offensive Cyber Warfare." The Diplomat. January 18, 2017. Accessed August 12, 2019. https://thediplomat.com/2017/01/trump-and-offensive-cyber-warfare/
12. Gilbert, David. "Inside the Massive Cyber War between Russia and Ukraine." Vice. March 29, 2019. Accessed August 20, 2019. https://news.vice.com/en_us/article/bjqe8m/inside-the-massive-cyber-war-between-russia-and-ukraine.
13. Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Wired. December 07, 2018. Accessed August 20, 2019. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
14. Grigsby, Alex. "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased." Council on Foreign Relations. November 15, 2018. Accessed August 20, 2019.

https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.
15. “International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms.” Just Security, June 28, 2018. Accessed August 8, 2019. https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.
16. Karagiannopoulos, Vasileios, and Mark Leiser. “Cyber Attacks Are Rewriting the 'Rules' of Modern Warfare – and We Aren't Prepared for the Consequences.” The Conversation, August 6, 2019. Accessed August 28, 2019. http://theconversation.com/cyber-attacks-are-rewriting-the-rules-of-modern-warfare-and-we-arent-prepared-for-the-consequences-117043.
17. Miralis, Dennis. “What Are Cyber Weapons? : Some Competing Definitions.” Lexology, September 28, 2018. https://www.lexology.com/library/detail.aspx?g=65179269-c85e-4253-a9a3-5d9ba1c9c906.
18. "Legal Review of Weapons and Cyber Capabilities." July 27, 2011. Accessed August 20, 2019. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-053.pdf.
19. Newman, Lily Hay. “What Israel's Strike on Hamas Hackers Means For Cyberwar.” Wired. Conde Nast, May 6, 2019. Accessed August 28, 2019 https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/.
20. Nkusi, Fred K. “AU Galvanises Cyber-Threats into Tougher Cybersecurity.” The New Times | Rwanda, July 29, 2018. Accessed August 30, 2019. https://www.newtimes.co.rw/opinions/au-galvanises-cyber-threats-tougher-cybersecurity.
21. Reuters. “France Has 3 Options for Those Mistral Warships It Was Going to Sell to Russia.” Business Insider. Business Insider, June 2, 2015. Accessed August 31, 2019. https://www.businessinsider.com/r-sink-or-sell-russia-spat-leaves-france-with-warships-to-spare-2015-6?IR=T.
22. Shackelford, Scott, and Indiana University. "What the World's First Cyber Attack Taught Us about Cybersecurity." World Economic Forum. November 5, 2018. Accessed August 20, 2019. https://www.weforum.org/agenda/2018/11/30-years-ago-the-world-s-first-cyberattack-set-the-stage-for-modern-cybersecurity-challenges.
23. Sharma, Nitin Mohan. “How a Piracy Protection Software Turned into a First Computer Virus.” Thrive Global, August 30, 2017. Accessed August 12, 2019. https://thriveglobal.com/stories/how-a-piracy-protection-software-turned-into-a-first-computer-virus/.
24. Shaw, Malcolm. “International Law.” Encyclopædia Britannica. Encyclopædia Britannica, inc., n.d. https://www.britannica.com/topic/international-law.
25. Stevens, Tim. “Cyberweapons: Power and Governance of the invisible”. October 2017. Accessed August 28, 2019.https://www.researchgate.net/publication/320293035_Cyberweapons_power_and_the_governance_of_the_invisible
26. "Tallinn Manual 2.0 on the International Law Applicable to Cyber." National Security Archive. April 24, 2019. Accessed August 20, 2019. https://nsarchive.gwu.edu/news/cyber-vault/2019-04-24/tallinn-manual-20-international-law-applicable-cyber-operations.
27. “The Cyber Law of War.” The State of Security, January 30, 2018. https://www.tripwire.com/state-of-security/featured/cyber-law-war/.

28. “The Global Trend Toward Cyber Sovereignty.” Endgame, October 2, 2018. Accessed August 30, 2019. https://www.endgame.com/blog/technical-blog/global-trend-toward-cyber-sovereignty.
29. “The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack.” Yale Law School, n.d. https://law.yale.edu/sites/default/files/area/center/global/document/2017.05.10_-_law_of_attribution.pdf.
30. “The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased.” Council on Foreign Relations. Council on Foreign Relations, n.d. Accessed September 2, 2019. https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.
31. “The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?” Lawfare, July 4, 2017. Accessed August 28, 2019.
32. Tom Uren, Bart Hogeveen and Fergus Harson, "Defining Offensive Cyber Capabilities", *Aspi.Org.Au*, 2018, https://www.aspi.org.au/report/defining-offensive-cyber-capabilities.
33. Wallace, David. "Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis." Accessed August 20, 2019. https://ccdcoe.org/uploads/2018/10/TP-11_2018.pdf.
34. Wilson, Clay. "Cyber Weapons: 4 Defining Characteristics." GCN. June 4, 2015. Accessed August 20, 2019. https://gcn.com/articles/2015/06/04/cyber-weapon.aspx.