Forum: General Assembly 1

Student Officer(s): Donghyun Han

TOPIC 1: The question of the implications of cyber and ABC weapons defense research

LibGuide

I. Introduction to the Topic

Weapons have existed and developed with humanity, with its purpose also evolving. Initially, weapons allowed humans to be more effective, whether hunting or self-protection. Slowly, however, they became tools for war and human conflict. In today's society, weaponry has become more lethal and powerful. As a result, many nations have been conducting more defense research into modern technology like cyber and ABC (atomic, biological, chemical) weapons. The fast-paced development of such weapons demands attention at the international, regional, and national levels (Stevens). Particularly because there's a lack of guidelines both internationally and domestically on new forms of weapons, there is a necessity for the establishment of cybersecurity and ABC weapon norms.

Currently, there have been several measures taken by the international community and the UN to control the spread of ABC like the Nuclear Non-proliferation Treaty (NPT) to control the spread of ABC and cyber weapons and the creation of the Biological Weapons Convention (BWC). However, these emerging weapons have garnered more attention because they have wide wide-reaching impact. For instance, defense research in cyberspace is especially crucial because all nations share it to a certain degree. So defense research at a global scale can lead to a successful framework to prevent further weapon development and stop deeper warfare.

Regionally, different areas may have varying preparation and resources to combat ABC and cyber weapons, leading to vulnerability. As countries share a certain land, neighboring nations not only share cyberspace but the nearby land as well. So, a physical attack on one nation can threaten another as well. Also, certain regions are already challenged with historical tensions and ongoing conflicts that heighten the concern for defense research. Ultimately, there must be a level of regional stability through joint exercises, information sharing, and coordinated response mechanisms (U.S. Department of Homeland Security).

For individual countries, defense research entails identifying weaknesses in their cyber security along with military technology. National policies, strategic alliances, and the creation of defense appliances can also impact the direction of a country's research. Also, there are ethical considerations surrounding research as defensive measures against lethal weapons like atomic bombs must still adhere to basic international norms. Simultaneously, technological advancements in research must be used strictly for defense capabilities, requiring a careful balance between ethical and realistic obstacles.

Within local communities, the implications of defense research revolve around ensuring citizens' safety and privacy. Cyberattacks can directly harm citizens leading to massive problems like data leaks. Similarly, a fallout involving the use of ABC weapons threatens the life and stability of everyone living in a set region (Georgetown Law). To promote domestic security, then, further efforts to spread awareness and community-based resilience activities have been conducted.

II. Definition of Key Terms & Concepts

ABC Weapons: ABC weapons stand for atomic, biological, and chemical weapons (Oxford References). These are weapons of mass destruction that can cause significant harm to the entire area where these arms are deployed. This term itself is in the name of the topic because these weapons classify some of the most lethal and harmful weapons that countries have access to.

Cyber Security: Cybersecurity is the practice and research into protecting a nation's networks, systems, and digital data from unauthorized access (CISA). Considering the question of defense research, preventing cyber threats is a major part of country safety especially because it's a rising way of warfare.

Defense Research: Defense Research is the investigation and development of technologies, strategies, and methodologies to prevent potential offenses in conflict (OEC). Specifically for this debate, defense research can entail any study into ways to stop or mitigate the harms of ABC and cyber attacks.

III. Key Stakeholders

United Nations: The United Nations is an intergovernmental organization to ensure global peace and prosperity. The UN plays a crucial role in connecting different countries and creating universal guidelines. For defense research, the UN may help fund and find new measures that individual countries can't handle.

Nuclear States: Nuclear states are countries with atomic weapons. Currently, 9 countries have access: Russia, the U.S., China, France, the U.K., Pakistan, India, Israel, and North Korea (ICAN). Knowing and understanding the positions of these countries is important because their decisions with nuclear weaponry can lead to immense harm to receiving nations, and even lead to nuclear warfare. Also, when conducting defense research for nuclear weapons, nuclear states have better positions to find measures.

International Committee of Red Cross: The ICRC is a humanitarian organization that provides assistance to areas in conflict while upholding international doctrines (ICRC). They play a key role with defensive research because they have created international guidelines like the International Humanitarian Law (IHL) that could ethically and legally limit the countries from indulging in certain research.

IV. Key Issues including Background Information

Arms Race in Cyberspace: The rapid growth of cyber capabilities amongst countries has led to an arms race in cyberspace. For many advanced countries, they have invested in creating cyber tools both in the defensive and offensive sectors. However, because the country's dependence on the internet increased, cybersecurity has become more important. As a result, there's a fear of opposing nations attempting to gain valuable information and country access via cyberspace. So, many countries have been in a race to develop faster and stronger ways to attack other nations to protect themselves. Addressing this underlying competition is urgent to prevent the escalation of cyber attacks.

Lack of International Framework: In the status quo, there is an absence of a universal framework to govern cyber and ABC weapons. The rapid changes in arms development have already bypassed previous international agreements. For instance, the NPT can prevent nuclear proliferation but doesn't account for other variations of weapons of mass destruction. So, there's a need for governments to come to a new agreement. The multi-faceted nature of cyber and ABC weapons that must be discussed includes humanitarian, ethical, and realistic perspectives.

Civilian Vulnerability: Civilian vulnerability is another key issue. Given the problem of various offensive developments, defensive research must advocate for citizen's safety. However, this may be challenging because it adds to the already challenging task of keeping up with unknown offensive threats. Nations must find a balance between national security and civilian safety because, when defensive measures account for civilian casualties, they may be more passive and less decisive.

V. Timeline of Resolutions, Treaties, and Events

Date	Description of event
1972	The Biological Weapons Convention (BWC) marked a step for the international community to stop the development of biological weapons that can harm all civilians and third parties in non-conflict.
1988	Iraqi government uses chemical weapons against Kurdish city amidst war (PBS).
2004	The development of the United Nations Group of Governmental Experts on Information Security (UNGGE) was established in 2004 by the General Assembly to strengthen cyber peace internationally.
2010	Stuxnet Attack showed a major cyberattack on Iran's nuclear facilities that showed the power of cyberattacks and the potential link between physical and cyber attacks.
2016	The Organization for the Prohibition of Chemical Weapons (OPCW) announced the destruction of chemical weapons destruction in Libya
2020	Several US government agencies were attacked during the SolarWind cyberattack. This may have caused sensitive information to be exfiltrated, which threatens the security of the impacted agencies.
2022	Several international discussions are held between research institutes, governments, and other organizations on the limitations and regulations for defense research.

2023	Declared chemical weapons are all destroyed, leading to less threat with chemical weaponry (OPWC).

VI. Possible Challenges & Solutions

Arms Race in Cyberspace: Currently, there is a cycle of competition in cyberspace. Countries rely more on it for their function, making it a potential weakness. In some sense, the countries seeking better offense can be a way to defend themselves due to mutual safety, this perspective can lead to escalating tensions, creating a situation similar to nuclear umbrellas. So, stakeholders should advocate for some form of international agreement to limit cyberattacks. While the specifics must be further discussed, this treaty can hold several clear limitations to the weaponization of the online world. Meanwhile, international organizations like the UN can advocate for transparency and diplomatic negotiation to ensure peace measures are upheld.

Lack of International Framework: As weapon technology has evolved past pre-existing international guidelines, new preventative measures need to be found. However, the process of creating a universal agreement can be challenging. With the new forms of weapons and relatively new cyberspace, more experts and research must be conducted to ensure all countries get a fair result from the treaty. Though there can be multiple approaches to solving the question of international frameworks against ABC and cyber threats, three key components are information sharing, defined limits, and engagement of non-state actors. Through information sharing, countries can recognize each other's limits and strengths, producing cooperation. Also, defining limits on the development of weaponry and defense research can lead to a safer future. Finally, engaging responsible third parties can ensure the fairness of this process.

National Sovereignty: Regarding cyberspace and ABC weapons, a question of national sovereignty emerges. Undoubtedly, certain nations may want to prioritize their autonomy and defense research arguing that cyber security along with national privacy depends on keeping their research and internal systems away from external interference. However, this perspective can damage international alliances and leave certain areas vulnerable, even stopping potential joint defense efforts and information sharing. So, to convince these nations while respecting their sovereignty, thoughtful policies to mandate a certain degree of privacy and domestic respect need to be made.

VII. Recommendations for Resolution Writing including Research

When a delegate writes a resolution, they should be mindful of both their country's stance and the supporting nations. Simultaneously, they should be aware of specific NGOs and international organizations that can support the fundamental solutions of the resolution. Also, they should remember to consider international treaties and pre-existing organizations that can either be repetitive or contradict their stance. Finally, delegates must be aware that the purpose of a resolution is to allow all member nations to effectively solve a certain issue, so solutions can't be too specific and country-focused.

A low-income country might view this issue as seeking international assistance to build its capacity regarding education and training programs and the development of technologies. This may be done by receiving financial and technological assistance from developed countries or international organizations.

Countries that prioritize their self-defense and sovereignty above the international agreement of the ABC weapons may approach this issue more subtly, as they may consider certain policies as a threat to their sovereignty. Thus, it is important for the delegates to determine the motivation behind opposing certain treaties or policies. In dealing with these countries, other nations may promote and establish responsible state behavior. This can be done by setting regulations on engagement in addressing the use of these weapons. However, it is very important to acknowledge and respect a certain level of the sovereignty of these nations as forcing these nations to engage in very restricting policies may disrupt international alliances, and stop potential joint force defenses and information sharing, which may heighten the risk as the state would be isolated.

VIII. Bibliography

CISA. "What Is Cybersecurity?" *Cybersecurity and Infrastructure Security Agency CISA*, 1 Feb. 2021, www.cisa.gov/news-events/news/what-cybersecurity.

"Connect the Dots on State-Sponsored Cyber Incidents - Stuxnet." *Council on Foreign Relations*, July 2010, www.cfr.org/cyber-operations/stuxnet.

Davenport, Kelsey. "Nuclear Weapons: Who Has What at a Glance | Arms Control Association." *Arms Control Association*, June 2023, www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat.

"Detail View." *DENIC Internet Governance Radar*, internet-governance-radar.de/en/about/institutions/detail-view/ungge-united-nations-group-of-governmental-experts-on-information-security-1. Accessed 30 Dec. 2023.

"DETER | Homeland Security." *Www.dhs.gov*, www.dhs.gov/science-and-technology/deter. Accessed 30 Dec. 2023.

Hollander, Rachelle. "Military & Defense Research Subject Aid | Online Ethics." *Onlineethics.org*, 2017, onlineethics.org/cases/oec-subject-aids/military-defense-research-subject-aid.

"International Committee of the Red Cross." *International Committee of the Red Cross*, 31 Aug. 2016, www.icrc.org/en.

"Nuclear Weapons and Warfare." *Www.rand.org*, www.rand.org/topics/nuclear-weapons-and-warfare.html.

Schneider, Barry R. "Biological Weapon." *Encyclopædia Britannica*, 27 Nov. 2017, www.britannica.com/technology/biological-weapon.

Stevens, Tim. "Cyberweapons: An Emerging Global Governance Architecture." *Palgrave Communications*, vol. 3, no. 1, 10 Jan. 2017, https://doi.org/10.1057/palcomms.2016.102.

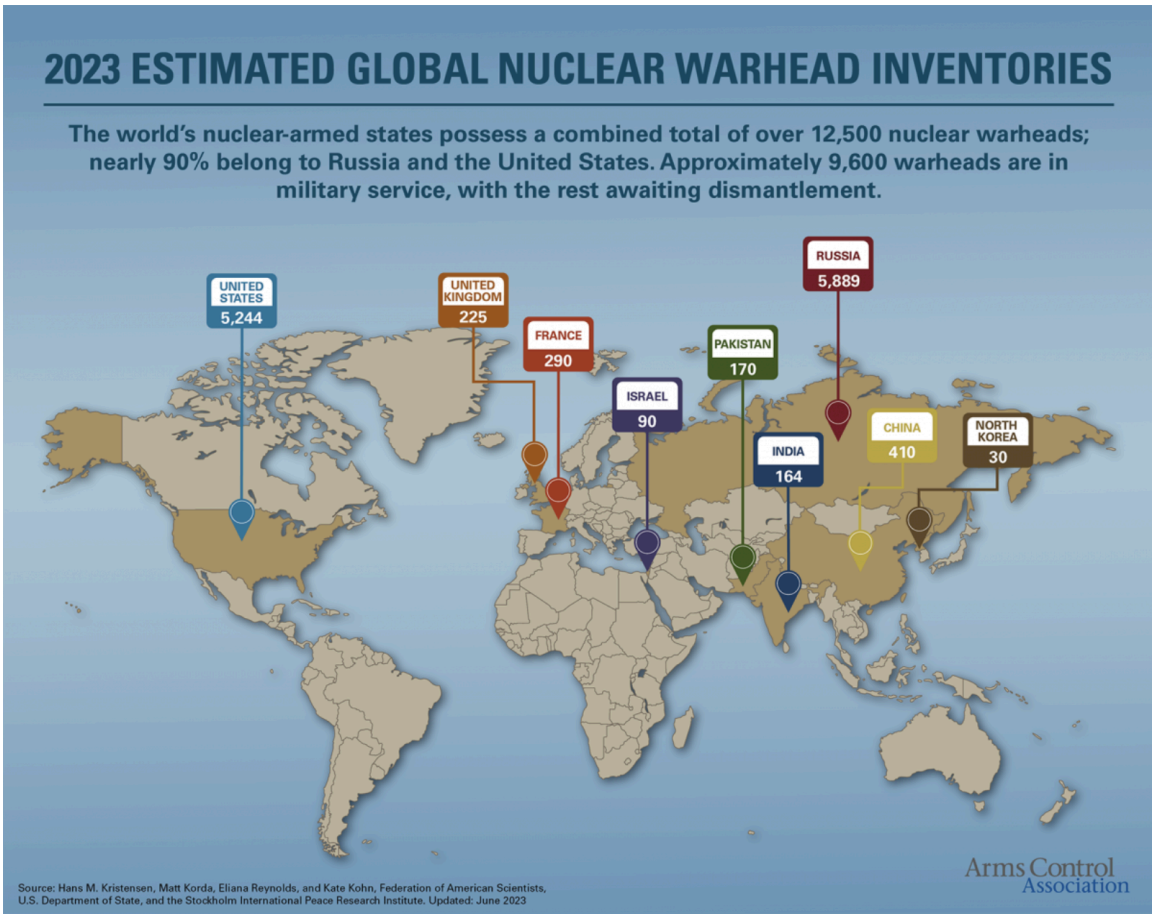
Sussman, Bruce. "Top 10 Most Powerful Countries in Cyberspace." *Www.secureworld.io*, 10 Sept. 2020, www.secureworld.io/industry-news/top-10-most-powerful-countries-in-cyberspace.

"The World's Nuclear Weapons." *ICAN*, 2023, www.icanw.org/nuclear_arsenals.

U.S. Department of State. "Nuclear Non-Proliferation Treaty - United States Department of State." *United States Department of State*, 2018, www.state.gov/nuclear-nonproliferation-treaty/.

United Nations. "Biological Weapons Convention – UNODA." *United Nations*, disarmament.unoda.org/biological-weapons/#:~:text=The%20Biological%20Weapons%20Convention%20(BWC.

IX: Additional Resources



Graph 1: NCPI 2020: Most Comprehensive Cyber Powers