Massachusetts Institute of Technology

Model United Nations Conference

Background Guide

Table of Contents

Letter from the Secretary General

Dear Delegates,

I am very excited to welcome you to Massachusetts Institute of Technology's 17th annual Model United Nations Conference - MITMUNC XVII! After months of planning, training and organizing, we hope this conference will be a new, challenging, and enriching experience for you.

With all the difficulties the world has experienced last year and is currently still experiencing, we still look forward to a brighter future. Building a sustainable future requires a lot of collaboration and effort and we are all hopeful to see that from you, the leaders of tomorrow.

This year, we decided to focus on technology and its impact on our societies and the whole world to test the pros and cons of technological advancement. Tech diplomacy is an important theme that defines MITMUNC XVII, especially with the prevalence of Artificial Intelligence. Technological advancements have paved the way for great and helpful solutions, yet they also opened up space for tech-abuse, which really makes us think, where are we heading? What's next? Dialogue, international relations and collaborations create the backbone of tech diplomacy and we are all looking forward to see your creativity spark during the conference to help implement tech diplomacy around the world, and fight technology-abuse that harms the international community.

Having experienced MITMUNC as a chair, then as a Secretary General, I am humbled and thrilled to guide MITMUNC into its best conference yet. Do not hesitate in contacting me or the secretariat team should you encounter any doubts along the way. I wish you the best of luck!

Sincerely,

Your Secretary General, Jad Abou Ali

For further inquiries, do not hesitate to contact us at sg-mitmunc@mit.edu.

MITMUNC XVII 2025

Letter from the Chairs

Dear Delegates,

Welcome to MITMUNC XVII!

Letter from Krystal:

My name is Krystal Jiang and I am so excited to be one of your co-chairs for DISEC. I've been involved in Model UN for 7 years, traveling around the East Coast to participate in regional and international MUN conferences and taking home awards for myself and my high school team. Over the years, I've had the privilege of experiencing MUN from all angles—competing, chairing, and even planning conferences. With this experience, I can confidently say you're in great hands for MITMUNC!

From my experiences, I know that Model UN has helped me with public speaking, writing, and research skills. Most importantly MUN has expanded my worldview not only through complicated topics and creative policies but meeting and interacting with people from all over the globe.

Outside of Model UN, I am a first-year student at MIT intending to major in architecture. As a result, I love art and often spend my free time painting, drawing, and sculpting. I am also into fashion and participate in MIT's fashion magazine: Infinite.

I hope you all gain new experiences and perspectives through this conference. I look forward to hearing about all the interesting solutions and ideas you all have in store.

Letter From Ryan:

Welcome to MITMUNC XVII! I'm Ryan Lin and I'm your other co-chair for DISEC. Unlike Krystal, I haven't had very much Model UN experience, so I'll be learning alongside you all at this conference. Even so, I know my stuff, so rest assured that this conference will run smoothly and professionally.

Outside of MUN, I'm a first-year student at MIT intending to double major in Finance and Mathematics. I love all things sports, and I was a captain of my high school's football, hockey, and track and field teams. I also currently play defensive back for the MIT football team. Some of my other

hobbies include Chinese yoyo, skateboarding, and magic: the gathering. I'm also into anime, with my favorite shows being Jojo's Bizarre Adventure, Attack on Titan, Mob-Psycho, Naruto, Yugioh, and Kaguya Sama: Love is War.

I hope y'all have a good time at MITMUNC this year! I look forward to hearing all the good ideas you all come up with!

We want to emphasize that DISEC is a beginner committee with the intention of being inviting and educational for new delegates. Thank you all for choosing DISEC as a part of your MUN journey, and we hope you enjoy the topics we have set out for you. We encourage you to use this as an opportunity to explore your interests, make mistakes, and meet new people. Lastly, we want you to remember that the "Best Delegate" is a delegate that can bring out the best in others. It is someone who works collaboratively and respectfully while diplomatically solving the world issues presented.

We can't wait to meet you all!

Sincerely,

Your Chairs: Krystal Jiang & Ryan Lin

For further inquiries, do not hesitate to contact us at disec-25@mit.edu

MITMUNC XVII 2025

Committee Introduction

The Disarmament and International Security Committee (DISEC), also known as the First Committee, was established in 1945 alongside the founding of the United Nations as one of its six main committees within the General Assembly. DISEC's primary mandate is to address issues of international security and disarmament under the scope of the UN Charter. Its central mission is to maintain global peace and security while promoting regulations on disarmament and fostering international stability. The committee's overarching goal is to strengthen nations without relying on excessive armament. (UN).

Since its inception after World War II to modern-day conflicts, DISEC has been involved in numerous landmark solutions has played a critical role in addressing some of the most pressing security challenges. In 1946, within the very first General Assembly Resolution, DISEC recommended the formation of a commission to examine the implications of atomic energy. This landmark resolution has set the precedent for DISEC's involvement in addressing global conflicts, issuing ceasefire directives, and supporting UN peacekeeping missions. (UN).

At this conference, delegates will deliberate on two pressing global issues: Regulation of cyber warfare and its impact on international security and Chemical And Biological Warfare. This committee will emphasize the consequences for nations employing emerging technologies and innovations to destabilize opposing nations and the urgent need for modern and adaptive solutions to address challenges posed by advancing technologies. Delegates should be encouraged to analyze current global issues and consider the far-reaching implications of the policies they propose.

Topic A: Regulation of cyber warfare and its impact on international security

I. Introduction

Cyber warfare, or the use of cyberattacks by nations or organized groups to damage, disrupt, or gain access to another nation's systems, has become one of the most pressing global security challenges in the 21st century. Cyberwarfare can be categorized in several ways: scale, intent, origin and targets. Some cyberattacks are small-scale, targeting individual systems, whereas others disrupt entire infrastructures, such as power grids or financial systems (UNSCEB). Intent refers to the goals of attacks, some cyberattacks are acts of espionage designed to gather intelligence, while others are destructive, aiming to paralyze critical systems or sow public chaos. The origins of cyber attacks are important as some attacks are state-sponsored, while others originate from independent hackers or extremist groups. Lastly, cyber warfare can be classified by its targets, ranging from military assets to civilian infrastructures like hospitals or communication networks.

Regardless of its form, cyberwarfare poses a multitude of threats. One of the most apparent is the potential for attacks to cripple essential services, causing widespread disruption to civilian life. For example, a coordinated cyberattack on a nation's power grid may result in blackouts, economic instability, and even loss of life. Another significant risk is the proliferation of cyber capabilities, where advanced tools and methods used in state-sponsored attacks may be reverse-engineered and used by non-state actors or hostile entities.

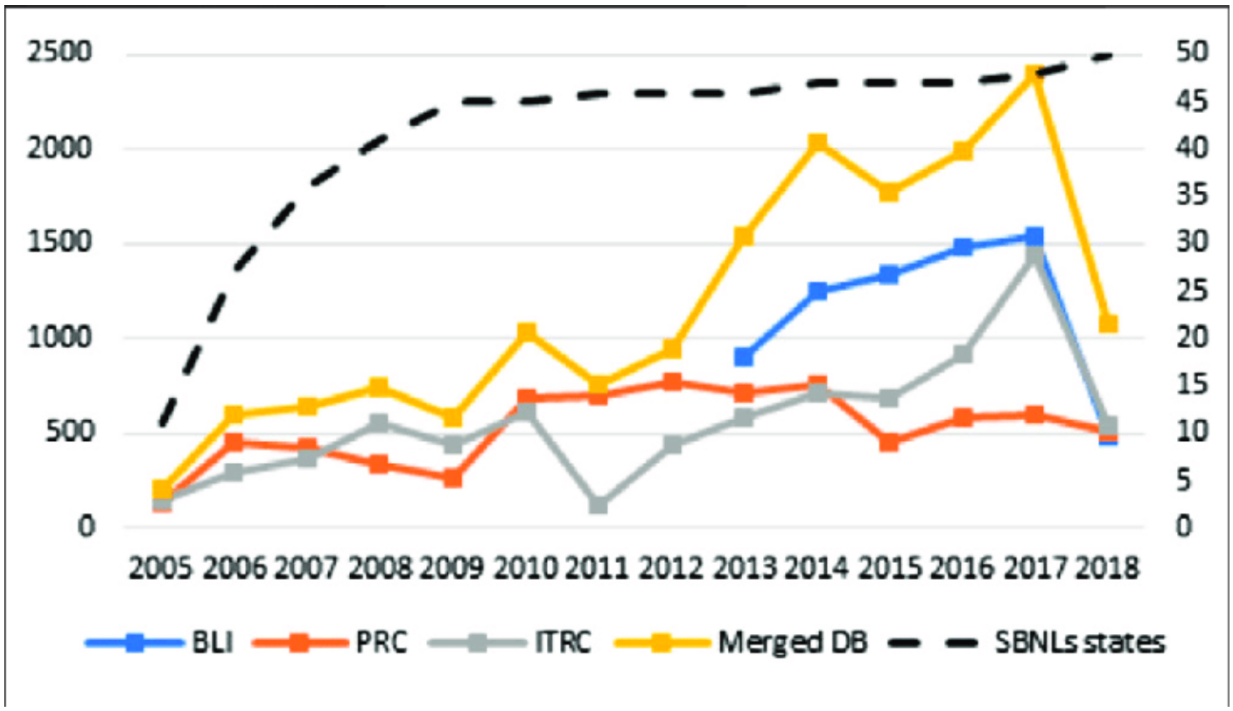
Moreover, the global nature of the internet creates a unique challenge: attacks originating in one nation can affect others across borders, making it difficult to attribute responsibility and coordinate responses.

While nations have proposed numerous measures to address the risks posed by cyber warfare, including international agreements and norms of behavior in cyberspace, these efforts are hampered by

mistrust and conflicting interests. Additionally, the dual-use nature of many cyber tools—capable of both defensive and offensive applications—complicates regulatory efforts, as nations seek to preserve their own capabilities while limiting the actions of adversaries. Developing robust frameworks for regulating cyber warfare and enhancing cybersecurity is critical, as the potential consequences of inaction could lead to cascading global crises in the event of a major cyber conflict.

II. History

1. Foundations of Cybersecurity



| Yearly reported number of cyber attacks by database and number of United States adopting SBNLs-2005/2018.

Figure 1. *Merging Datasets of CyberSecurity Incidents for Fun and Insight. Frontiers in Big Data (Abbiati, et al).*

Cybersecurity and cyberwarfare have been large concerns since 1971 when American computer programmer Bob Thomas developed a virus that exposed areas of vulnerability and security flaws for what would be known as the internet. In response, the first cybersecurity measure was created by Ray Tomlinson to counteract Thomas' virus which set the tone for anti-

virus programs (Monroe Edu). With the internet becoming widely available the exponential growth of threats within the past 50 years has been felt by almost every nation and the potential for mass destabilization is not a dystopian concept. Thus, the United Nations is keen to protect against cyberterrorism and cyberwarfare. As seen in Monroe Edu, the types of cyberattacks include:

1. **Phishing Campaigns**: Phishing remains the most frequent method for initial access. Attackers target government employees to steal login credentials or infect systems.
2. **Advanced Persistent Threats (APTs):** APTs are extensively used by state-sponsored actors to infiltrate government systems, gather intelligence, or disrupt operations over time.
3. **Distributed Denial of Service (DDoS):** Governments frequently face DDoS attacks, especially during elections, protests, or periods of heightened political tension, to disable websites or services.
4. **Ransomware Attacks:** While less common than phishing or APTs, ransomware attacks targeting government systems have surged in recent years, causing significant disruptions.
5. **Malware Infections:** Malware, including trojans, worms, and spyware, is a staple in cyber-espionage and sabotage campaigns against governments.
6. **Critical Infrastructure Attacks:** Attacks on power grids, water systems, and other government-controlled infrastructure are increasingly common, aiming to destabilize essential services.
7. **Supply Chain Attacks:** Increasingly popular among sophisticated adversaries, these attacks infiltrate government systems via compromised third-party providers.

2. Past Cyberwarfare activity

Within the past 20 years, the Center for Strategic and International Studies (CSIS) has documented significant cyberattacks globally from 2003 to 2024. Many of these attacks are performed between a nation's governments and often are related to espionage and

destabilization of a nation's digital infrastructure. For instance, in 2005 China was known to have attacked the US Department of Defense's networks to target national security information such as weapons testing and design data. More recently, in 2017, the NotPetya malware attack—attributed to Russian actors—caused massive disruption across Ukraine, targeting critical infrastructure like banks, energy companies, and government systems. Though initially aimed at Ukraine, the attack spread globally, resulting in billions of dollars in damages. Similarly, the 2020 SolarWinds cyberattack, a sophisticated supply-chain attack, infiltrated several U.S. government agencies and private companies, with evidence pointing to a Russian-backed group. This breach underscored the vulnerabilities of interconnected systems and the potential scale of cyberwarfare (CSIS).

The global nature of cyberspace has led to numerous conflicts involving non-state actors as well. For example, the 2021 ransomware attack on Colonial Pipeline by the DarkSide group disrupted fuel supplies across the U.S. East Coast, highlighting the increasing role of independent criminal organizations in cyber warfare. These incidents illustrate the diverse motivations and targets of cyberattacks, ranging from state espionage to economic extortion (CSIS).

III. International Actions

1. Efforts Address Cyber Warfare

Despite these alarming developments, international efforts to regulate cyberwarfare have struggled to gain traction. The Budapest Convention on Cybercrime (2001) remains one of the few legally binding international agreements aimed at addressing cyber threats. It outlines a framework for international and private sectors to share experiences and foster productive relationships with technology. Additionally, it instructs nations to criminalize actions such as damaging, deleting, deteriorating, altering, or suppressing computer data without authorization, with the option to require that such actions result in serious harm to qualify as

offenses. The convention also mandates criminal liability for actions that hinder the functioning of computer systems or involve the misuse of devices, including unauthorized access codes or malicious tools. However, its focus on cybercrime rather than cyberwarfare limits its effectiveness in governing state-sponsored actions.

2. Open Ended Working Group on ICT

More recently, the Open-Ended Working Group (OEWG), established by the UN General Assembly in 2018, has sought to build consensus on cyber norms and confidence-building measures. In 2021, they published a new framework for nations to follow. The Open-Ended Working Group (OEWG) on Information and Telecommunications in the context of international security highlights the need for a secure and peaceful ICT environment to maintain international peace, stability, and development (UNOEWG). The report underscores threats posed by malicious ICT use, including risks to critical infrastructure and global connectivity. It emphasizes voluntary norms for state behavior, the applicability of international law, capacity-building, confidence-building measures (CBMs), and regular institutional dialogue. Recommendations include fostering cooperation, narrowing digital divides, enhancing cybersecurity frameworks, and continuing multilateral discussions to build consensus and implement effective ICT security measures (UNOCT). While progress has been made, significant disagreements remain, particularly between major powers such as the U.S., China, and Russia, who have differing views on sovereignty, attribution, and acceptable cyber operations (Khelif).

AI has also been a concern within the United Nations as they have recently created a High-Level Advisory Board on Artificial Intelligence with the goal of harnessing AI for humanity while also addressing its ethical concerns. In August of 2023 globally inclusive governance of AI was explored as experts were called upon from 128 nations. (Khelif).

IV. Countries' Positions

Adapted from Shutterstock

1. NATO Nations

Nations in North America, particularly those within NATO, have been significant victims of cyberwarfare and cyberattacks. NATO includes nations in North America and Europe. The United States has frequently been targeted by state-sponsored actors, particularly from China and Russia, with goals such as collecting sensitive data and conducting espionage on government officials and defense agencies. Between 2015 and 2022, the U.S. reported over 200 major cyber incidents, many of which involved breaches of government systems, including the infamous SolarWinds cyberattack in 2020 that infiltrated multiple federal agencies (SentinelOne).

Although these attacks often focus on intelligence gathering over direct harm to civilians, their potential consequences are far-reaching. Stolen data could facilitate advancements in weapons development, disrupt critical infrastructure, or be used for misinformation campaigns during elections. For example, during the 2016 U.S. presidential election, Russian hackers reportedly attempted to influence public opinion and undermine democratic processes (FBI).

NATO has identified cyber defense as a core task of collective defense. In 2016, it formally recognized cyberspace as an operational domain, alongside land, sea, and air. The alliance's Cyber Defense Pledge, adopted in 2016, commits member nations to strengthening their national cyber defenses and enhancing cooperation. NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE), based in Estonia, plays a central role in training and sharing expertise (CCDCOE).

2. BRICS Nations

The BRICS nations—Brazil, Russia, India, China, and South Africa—have diverse cyber capabilities and approaches to cybersecurity. Some member states are among the most advanced in cyber offense and defense, while others face significant challenges in securing their digital ecosystems.

Russia and China, in particular, are often accused of conducting sophisticated cyber operations, including state-sponsored attacks targeting governments and corporations globally. For example:

Russia: The NotPetya attack in 2017 caused over $10 billion in damages worldwide, with its origins linked to Russian state actors. (Greenberg)

China: The APT10 group, associated with the Chinese government, has been implicated in global cyberespionage campaigns targeting intellectual property and trade secrets.

India, on the other hand, has been a frequent target of cyberattacks. A 2021 report revealed that India faced over 18 million cyberattacks in the first quarter alone, with a significant portion originating from China and Pakistan (Meszaros). Brazil and South Africa have also seen a rise in ransomware attacks and financial fraud, driven by the expansion of digital services in these nations.

Despite these challenges, BRICS members recognize the importance of cooperation in addressing cyber threats.

V. Projections and Implications

Dealing with cyberterrorism is crucial because it directly threatens global stability, public safety, and economic resilience. Cyberattacks on essential infrastructure, such as energy grids, healthcare systems, and financial networks, can cause widespread disruption, undermine trust in governments, and endanger lives. Moreover, the borderless nature of cyberspace means the impact of such attacks often transcends physical boundaries and borders and can destabilize entire regions.

Failing to address cyberterrorism could escalate conflicts, enable terrorist organizations to grow in strength, and increase vulnerabilities in critical systems worldwide. International cooperation to strengthen cybersecurity, share intelligence, and establish clear norms of behavior is vital to safeguarding global peace, fostering resilience, and ensuring the security of our interconnected world.

VI. Conclusion

As cyberwarfare continues to evolve, the potential consequences of inaction are increasingly dire. The rapid development of artificial intelligence and quantum computing could amplify the scope and impact of future cyberattacks. To address this, the international community must prioritize creating enforceable frameworks that balance national security interests with global stability. The regulation of cyberwarfare and the establishment of resilient cybersecurity measures are no longer optional but essential for safeguarding the digital and physical infrastructure of nations worldwide. As the secretary general of the United Nations Office of Counter-Terrorism Vladimir Voronkov says "We must come together now and we must do it fast to mitigate this threat and ensure that new technologies remain a force for good rather than a force for evil"

VII. Questions to be Addressed

- How should the international community address continual violations?
- Can a binding international treaty on cyberwarfare be effectively enforced, considering the challenges of attribution and sovereignty?
- How can states balance the development of offensive cyber capabilities with maintaining global cybersecurity?
- How can developing nations be supported in building robust cyber defenses without creating dependencies on major powers? And should developed and wealthy nations be responsible for funding?
- How can the usage of AI help or hurt policies against cyber warfare? How should policy react?

VIII. Bibliography

2021 - Un-Arm - Military Expenditure, front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf. Accessed 5 Jan. 2025.

"The Attack on Colonial Pipeline: What We've Learned & What We've Done over the Past Two Years: CISA." Cybersecurity and Infrastructure Security Agency CISA, 23 Aug. 2024, www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

Belli, Luca. "Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation." The African Journal of Information and Communication, Authors, www.scielo.org.za/scielo.php?script=sci_arttext&pid=S2077-72132021000200008. Accessed 4 Jan. 2025.

"Budapest Convention - Cybercrime - Www.Coe.Int." Cybercrime, 8 Feb. 2024, www.coe.int/en/web/cybercrime/the-budapest-convention.

CyberBRICS, cyberbrics.info/. Accessed 4 Jan. 2025.

"Cybersecurity and New Technologies | Office of Counter-Terrorism." United Nations, United Nations, www.un.org/counterterrorism/cybersecurity. Accessed 4 Jan. 2025.

"Cybersecurity Community of Practice." CEB, unsceb.org/topics/cybersecurity. Accessed 4 Jan. 2025.

"Cybersecurity History: Hacking & Data Breaches." Monroe University, www.monroeu.edu/news/cybersecurity-history-hacking-data-breaches. Accessed 4 Jan. 2025.

Excerpt, Andy Greenberg. "The Untold Story of Notpetya, the Most Devastating Cyberattack in History." Wired, Conde Nast, 22 Aug. 2018, www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

"Group of Governmental Experts." United Nations Office for Disarmament Affairs, disarmament.unoda.org/group-of-governmental-experts/. Accessed 4 Jan. 2025.

"High-Level Advisory Body on Artificial Intelligence | Office of the Secretary-General's Envoy on Technology." United Nations, United Nations, www.un.org/techenvoy/ai-advisory-body. Accessed 4 Jan. 2025.

"High-Level Advisory Body on Artificial Intelligence | Office of the Secretary-General's Envoy on Technology." United Nations, United Nations, www.un.org/techenvoy/ai-advisory-body. Accessed 4 Jan. 2025.

Knight, Will. "The United Nations Wants to Treat AI with the Same Urgency as Climate Change." Wired, Conde Nast, 19 Sept. 2024, www.wired.com/story/united-nations-artificial-intelligence-report/.

Nato. "Cyber Defence." NATO, 4 Dec. 2024, www.nato.int/cps/de/natohq/topics_78170.htm.

"Open-Ended Working Group." United Nations Office for Disarmament Affairs, disarmament.unoda.org/open-ended-working-group/. Accessed 4 Jan. 2025.

"Peace and Security." United Nations, United Nations, www.un.org/en/global-issues/peace-and-security#:~:text=On%20many%20occasions%2C. Accessed 4 Jan. 2025.

"Significant Cyber Incidents: Strategic Technologies Program." CSIS, www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Accessed 4 Jan. 2025.

"Top 7 Cyber Attacks in the United States." SentinelOne, 12 Dec. 2024, www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-attacks-in-the-united-states/#:~:text=Russian%2DLinked%20Global%20Cyberattack%20.

U.S. Department of State, U.S. Department of State, www.state.gov/reports/country-reports-on-terrorism-2021/. Accessed 4 Jan. 2025.

"United Nations AI Resolution: A Significant Global Policy Effort to Harness the Technology for Sustainable Development: Iheid FC." Title=, executive.graduateinstitute.ch/communications/news/united-nations-ai-resolution-significant-global-policy-effort-harness#:~:text=On%2021%20March%2C%20the%20United,human%20rights%20and%20international%20law. Accessed 4 Jan. 2025.

"United Nations General Assembly First Committee." Wikipedia, Wikimedia Foundation, 26 Nov. 2024, en.wikipedia.org/wiki/United_Nations_General_Assembly_First_Committee.

Topic B: Strengthening Biological and Chemical Weapons Convention and Reparations

I. Introduction

Photo adapted from Shutterstock

Chemical Warfare:

A Brief Overview of Chemical Warfare: Chemical warfare is the weaponization of toxic chemicals to cause intentional injury and death to humans. Throughout history, humans have engaged in chemical warfare with some of the earliest occurrences involving poisoned arrows and spears. Chemical weapons were mainly popularized by Germany during World War I (1914-1918) with the initial usage of Chlorine bombs at the Second Battle of Ypres (Belgium 1915). Chlorine was followed by the introduction of Phosgene and Mustard Gas which sparked an era of chemical weapons research

following the war. In 1925, the Geneva Protocol sought to prohibit chemical warfare, but weapons research continued. Chemical Warfare was limited during World War II (1939 - 1945), due to concern over their devastating impacts, but poison gases were utilized by the Nazis in their concentration camps. During the Cold War, the United States and The Soviet Union enhance chemical weapons research, stockpiling enough weaponry to wipe out all life. Following the Cold War, in 1993, The Chemical Weapons Convention (CWC) was signed completely eradicating the use and storage of chemical weapons. Following the CWC, most chemical weapon stockpiles have been destroyed, but there has still been usage by the Syrian Government during the Syrian Civil War (Everts).

Types of Weapons

Nerve agents are some of the most dangerous chemical weapons. They disrupt the nervous system by blocking the transmission of nerve signals. Common nerve agents include sarin, VX, and soman. Exposure to these substances can cause convulsions, breathing difficulties, and death (OPCW).

Blood agents work by stopping the body from using oxygen, effectively causing suffocation. These agents act quickly, usually after being inhaled. Common blood agents include hydrogen cyanide and cyanogen chloride (OPCW).

Blister agents or vesicants, cause painful blisters and burns on the skin and can damage the respiratory system if inhaled. Examples of blister agents are mustard gas and lewisite. These weapons often leave victims with long-lasting injuries and can be fatal (OPCW).

Choking agents damage the respiratory system. Victims often experience choking, coughing, and fluid buildup in the lungs (pulmonary edema). These agents are often released as gases, making them especially dangerous in confined spaces where they can cause widespread harm. Examples include chlorine and phosgene (OPCW).

Riot control agents, commonly referred to as tear gas, are less lethal but still cause significant discomfort. They are used primarily for crowd control and law enforcement. These agents irritate the eyes, nose, and respiratory system, leading to temporary pain and incapacitation (OPCW)

Biological Warfare:

Overview:

Biological weapons are tools of warfare and terrorism that use living organisms, such as bacteria, viruses, or toxins, to cause disease, death, and disruption. These weapons are designed to target humans, animals, or crops, with the goal of creating mass casualties, economic damage, or societal panic. The effects of biological weapons can be far-reaching and difficult to control, as they often spread beyond the intended target, affecting entire populations and ecosystems. The use of biological weapons poses unique challenges due to their stealthy nature. Unlike conventional weapons, biological agents are often invisible, odorless, and tasteless, making their deployment difficult to detect until symptoms appear. Furthermore, the effects of biological attacks can be delayed, as diseases may take days or weeks to incubate, complicating response efforts and containment. This delay allows diseases to spread widely, creating larger outbreaks and increasing the number of affected individuals. International efforts to prevent the development and use of biological weapons are anchored in the Biological Weapons Convention (BWC), which signed in 1972 prohibits the production, stockpiling, and use of biological and toxin weapons. However, challenges remain in enforcing compliance and addressing advancements in biotechnology that could be misused for weaponization. (Schneider)

Types of Weapons:

Bacterial Agents

Bacterial agents are living microorganisms that cause diseases in humans, animals, or plants. These agents can be dispersed in the air, water, or food and are capable of causing widespread illness and death. Bacteria-based biological weapons are particularly concerning because many bacterial infections

can spread from person to person, further amplifying their impact. Examples include Bacillus anthracis, which causes anthrax, and Yersinia pestis, the bacterium responsible for plague. (Schneider).

Viral Agents

Viruses are highly infectious pathogens that can cause severe and often fatal diseases. Viral agents are especially dangerous because of their ability to mutate, making them resistant to treatments or vaccines, and their capacity to cause pandemics. Examples include the smallpox virus, which has a high fatality rate and can spread rapidly through populations, and hemorrhagic fever viruses, such as Ebola, which cause severe internal bleeding and organ failure (Schneider).

Toxins

Toxins are poisonous substances produced by living organisms, such as bacteria, fungi, or plants. Unlike bacterial or viral agents, toxins are not alive and cannot reproduce, but they are extremely potent. Even small amounts of these substances can be lethal, making them effective biological weapons. Examples include botulinum toxin, produced by Clostridium botulinum, which can cause paralysis and death, and ricin, derived from castor beans, which can disrupt cell function and cause organ failure (Schneider).

II. History

Photo adapted from Shutterstock

1. Chemical Warfare

Chemical warfare, the use of toxic chemical substances as weapons, has a history dating back to ancient times, when armies would poison wells or use noxious fumes to harm enemies. However, its modern form emerged during World War I, where chemicals like chlorine, phosgene, and mustard gas were deployed on a large scale, causing horrific injuries and deaths. Despite the Geneva Protocol of 1925 banning the use of chemical weapons, they were used sporadically in conflicts, such as by Italy in Ethiopia (1930s), Japan in China (1930s-40s), and Iraq during the Iran-Iraq War (1980s). The 20th century saw efforts to curb their use, culminating in the Chemical Weapons Convention (CWC) of 1993, which prohibits the

development, production, stockpiling, and use of chemical weapons. Despite these measures, instances of their use have persisted, highlighting ongoing challenges in eliminating chemical warfare (Everts).

2. Timeline

600 BCE: The Athenians poison Kirrha's water supply with hellebore plants.

479 BCE: Sulfur fumes are used by Peloponnesian forces against Plataea.

1675: The Strasbourg Agreement outlaws poisoned bullets.

1845: French troops use smoke to kill Berber tribespeople in Algeria.

1861–1865: Chemical weapons are proposed but not implemented during the American Civil War.

1914–1918 (World War I): Chemical weapons like chlorine and mustard gas cause over 1.3 million casualties, with significant events including the first large-scale use at Ypres (1915) and the introduction of mustard gas (1917).

1925: The Geneva Protocol bans the use of chemical and biological weapons but permits stockpiling.

1935–1936: Italy uses mustard gas in Ethiopia.

1936: German chemist Gerhard Schrader synthesizes tabun, the first nerve agent.

1939–1945 (World War II): Poison gases are used in Nazi concentration camps, but not on European battlefields.

1961–1971: The U.S. uses napalm and Agent Orange during the Vietnam War.

1980s: Iraq uses chemical weapons during the Iran-Iraq War and against Kurds, while Iran begins its own program.

1993: The Chemical Weapons Convention (CWC) bans chemical weapons globally.

2013: Sarin gas is used by the Syrian military, leading to international condemnation and partial disarmament

3. Biological Warfare

Biological warfare dates to ancient times, with early examples including the use of poisoned water and disease-infected bodies in sieges. In the 18th century, smallpox-infected blankets were used against Native Americans, and during World War I, nations experimented with biological agents like anthrax. World War II saw further development, particularly by Japan's Unit 731, but biological weapons were not widely deployed in combat. The 1972 Biological Weapons Convention banned such weapons, though the U.S. and Soviet Union continued research during the Cold War. In modern times, bioterrorism concerns, such as the 2001 anthrax attacks (Frischknecht).

4. Timeline

1155: Emperor Barbarossa poisons water wells with human bodies, Tortona, Italy.

1346: Mongols catapult bodies of plague victims over the city walls of Caffa, Crimean Peninsula.

1495: Spanish mix wine with blood of leprosy patients to sell to their French foes, Naples, Italy.

1650: Polish fire saliva from rabid dogs towards their enemies.

1675: First deal between German and French forces not to use 'poison bullets'.

1763: British distribute blankets from smallpox patients to Native Americans during Pontiac's Rebellion.

1797: Napoleon floods the plains around Mantua, Italy, to enhance the spread of malaria.

1863: Confederates sell clothing from yellow fever and smallpox patients to Union troops, USA.

May 7, 1763: British soldiers distribute smallpox-infected blankets to American Indian tribes during Pontiac's Rebellion.

1940: Japan's Ping Fan biological weapons complex starts operations, conducting inhumane experiments (Unit 731)

November 18, 1941: U.S. biological weapons investigation committee formed.

January 2, 1942: Churchill approves production of anthrax-laced cattle cakes.

August 1945: Unit 731 is destroyed as Russians advance.

April 2, 1979: Soviet Union's accidental anthrax release kills 70 people.

March 16, 1988: Iraq uses chemical weapons against Kurdish cities.

October 15, 2001: Anthrax attacks occur in the U.S.

March 2003: The U.S. invades Iraq, on the basis the Iraq holds biological weapon stores

III. International Actions

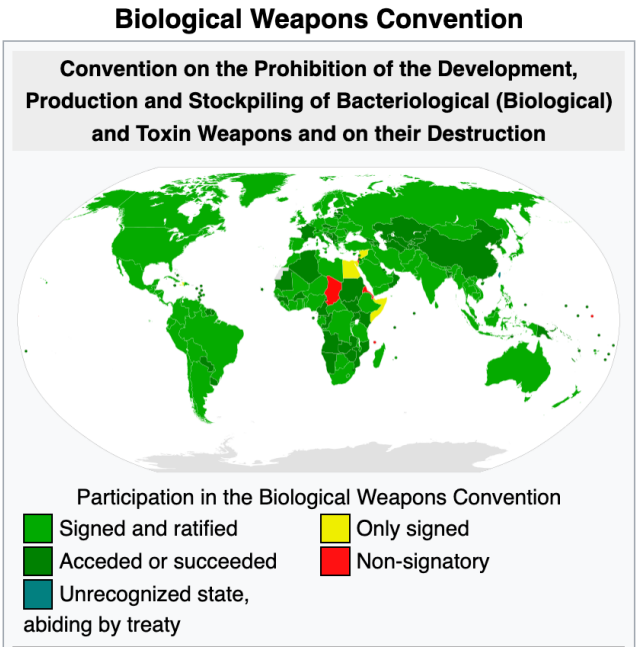
1. Use Geneva Protocol (1925)

The Geneva Protocol of 1925, formally known as the Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, is an international treaty that prohibits the use of chemical and biological weapons in armed conflicts. Signed on June 17, 1925, and entering into force on February 8, 1928, the protocol emerged in response to the widespread use of chemical weapons during World War I, which caused devastating casualties and long-term suffering. While the treaty bans the use of such weapons, it does not prohibit their production or stockpiling, a loophole later addressed by subsequent treaties such as the Chemical Weapons Convention (1993) and the Biological Weapons Convention (1972). The Geneva Protocol has been a cornerstone of international efforts to limit the inhumane methods of warfare and has been ratified by most nations, although its enforcement relies on collective international will (Geneva Protocol).

"Whereas the use in war of asphyxiating, poisonous or other gases, and of all analogous liquids, materials or devices, has been justly condemned by the general opinion of the civilized world; and Whereas the prohibition of such use has been declared in Treaties to which the majority of Powers of the world are Parties; and To the end that this prohibition shall be universally accepted as a part of International Law, binding alike the conscience and the practice of nations;"

2. Biological Weapons Convention (1972)

The Biological Weapons Convention (BWC), formally known as the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, is a key international treaty that seeks to eliminate biological and toxin weapons. Opened for signature in 1972 and entering into force on March 26, 1975, the BWC prohibits the development, production, acquisition, stockpiling, and transfer of biological agents or toxins intended for hostile purposes or armed conflict. It was the first treaty to ban an entire category of weapons of mass destruction, marking a significant step in disarmament and non-proliferation efforts. (Biological Weapons Convention).



MedLink Neurology: Participation in the Biological Weapons Convention

3. Chemical Weapons Convention (1993)

The Chemical Weapons Convention (CWC) of 1993 is a landmark international treaty that prohibits the development, production, acquisition, stockpiling, transfer, and use of chemical

weapons, as well as mandates their destruction. Adopted on January 13, 1993, and entering into force on April 29, 1997, the treaty represents a comprehensive effort to eliminate an entire category of weapons of mass destruction under strict international verification. Administered by the Organization for the Prohibition of Chemical Weapons (OPCW), the CWC establishes mechanisms for on-site inspections, monitoring, and reporting to ensure compliance. As of today, the vast majority of UN member states have joined the convention, collectively committing to the goal of a world free of chemical weapons. The treaty has led to the destruction of significant stockpiles of chemical weapons globally, though challenges remain in ensuring universal adherence and addressing alleged violations. (Chemical Weapons Convention).

"The Chemical Weapons Convention (CWC) prohibits the development, production, stockpiling and use of chemical weapons and requires the destruction of both chemical weapons production facilities and the weapons themselves.

The CWC strengthens the 1925 Geneva Protocol prohibition on the use of chemical weapons by prohibiting their use "under any circumstances". Chemical weapons are defined broadly as "toxic chemicals and their precursors, except where intended for purposes not prohibited", munitions exclusively designed for the delivery of toxic chemicals and other equipment designed for use with such munitions."

4. UNSC Resolution 1540 (2004)

United Nations Security Council Resolution 1540, adopted unanimously on April 28, 2004, aims to prevent the proliferation of weapons of mass destruction (WMDs) to non-state actors, including terrorist groups. The resolution obligates all UN member states to establish and enforce domestic controls to prevent the development, acquisition, transfer, or use of nuclear, chemical, and biological weapons, as well as their delivery systems, by non-state actors. It calls for states to strengthen legal and regulatory frameworks, enhance border controls, and improve international cooperation to combat WMD proliferation. Resolution 1540 also established a committee to monitor its implementation and

provide assistance to states needing support in meeting its requirements (United Nations Security Council).

IV. Countries' Positions

Several countries have been involved in the development, use, or stockpiling of chemical and biological weapons, often during times of war or as part of military research programs. During World War I, nations like Germany, France, and the United Kingdom deployed chemical weapons such as chlorine and mustard gas, causing widespread devastation. In World War II, Japan's Unit 731 conducted horrific biological warfare experiments, while Germany developed chemical agents but refrained from battlefield use. During the Cold War, the United States and the Soviet Union engaged in extensive research and stockpiling of chemical and biological weapons as part of their arms race. More recently, countries such as Iraq under Saddam Hussein used chemical weapons against civilians and during conflicts, including the Iran-Iraq War. Non-state actors like terrorist groups have also sought to acquire or use these weapons.

In recent times, despite the enactment of the CWC and BWC, several countries, including Syria, Russia, and North Korea, have been accused of violating these treaties. For instance, Syria has repeatedly been implicated in the use of chemical weapons during its civil war, despite being a CWC signatory. Chemical weapons were used in Malaysia in 2017 to assassinate Kim Jong-Un's half-brother Kim Jong-Nam. Russia has faced accusations of using chemical agents like Novichok in assassination attempts, such as the poisoning of Sergei Skripal in 2018 and Alexei Navalny in 2020. Non-state actors, including terrorist groups like ISIS, have also attempted to deploy chemical agents, raising concerns about the accessibility of such weapons to extremist organizations (Diplomatic Service of the European Union).

Continued efforts are needed to address these gaps and enhance global security against the threat of chemical and biological warfare.

V. Projections and Implications

The future of biological and chemical warfare presents significant challenges, as advancements in biotechnology, synthetic biology, and chemical engineering increase the potential for more sophisticated and accessible weapons. Emerging technologies could enable the creation of novel biological agents tailored to target specific populations or evade existing detection and treatment methods. Similarly, advances in chemistry might lead to the development of undetectable or rapidly acting chemical agents. The dual-use nature of these technologies—serving both civilian and military purposes—complicates efforts to monitor and regulate their misuse. The implications of such developments are far-reaching, including threats to global health, destabilization of international security, and the potential for catastrophic humanitarian crises. Non-state actors, such as terrorist groups, could exploit these technologies, increasing the likelihood of unconventional attacks. Potential danger highlights the need for robust international frameworks, improved verification mechanisms, and global cooperation to prevent the misuse of science while fostering its peaceful applications. Addressing these challenges is essential to safeguarding human security and upholding international norms against weapons of mass destruction (Darling, Noste).

VI. Conclusion

Addressing the threat of biological and chemical warfare requires a unified and proactive global effort. Strengthening international frameworks, enhancing verification mechanisms, and fostering transparency are critical to preventing the misuse of these devastating weapons. By prioritizing collaboration, innovation, and strict regulation, the global community can work together to ensure that scientific advancements are used for peace and progress, not destruction. The fight against these threats is not just about security but about safeguarding the future of humanity.

VII. Questions to be Addressed

- How can existing international frameworks, such as the Chemical Weapons Convention (CWC) and the Biological Weapons Convention (BWC), be strengthened to ensure compliance?
- What should be the consequences for nations found in violation of the CWC or BWC?
- How can the global community balance the promotion of scientific research with the prevention of its misuse for warfare?
- What measures can nations implement to prevent non-state actors, such as terrorist groups, from accessing chemical and biological weapons?
- What role can technology and innovation play in detecting and neutralizing chemical and biological threats?

VIII. Bibliography

1925 Geneva Protocol Text, media.nti.org/documents/1925_geneva_protocol_text.pdf. Accessed 5 Jan. 2025.

"Biological Weapon." *Encyclopædia Britannica*, Encyclopædia Britannica, inc., 30 Nov. 2024, www.britannica.com/technology/biological-weapon.

"Biological Weapons Convention." *Wikipedia*, Wikimedia Foundation, 26 Dec. 2024, en.wikipedia.org/wiki/Biological_Weapons_Convention.

"A Brief History of Chemical War." *Science History Institute*, 2 June 2023, www.sciencehistory.org/stories/magazine/a-brief-history-of-chemical-war/?gad_source=1&gclid=Cj0KCQiAst67BhCEARIsAKKdWOlGDAmD1uMi-Vvd0jY88eX41cBAPCxc-hVC3X9IKG5GWusbwvZpZ-kaAhk3EALw_wcB.

BWC-Text-English-1.Pdf, front.un-arm.org/wp-content/uploads/2020/12/BWC-text-English-1.pdf. Accessed 5 Jan. 2025.

"Chemical Weapons Remain a Threat to the World." *EEAS*, www.eeas.europa.eu/eeas/chemical-weapons-remain-threat-world_en. Accessed 4 Jan. 2025.

"Chemical, Biological, Radiological and Nuclear Terrorism | Office of Counter-Terrorism." *United Nations*, United Nations, www.un.org/counterterrorism/chemical-biological-radiological-nuclear-terrorism. Accessed 4 Jan. 2025.

Darling, Robert G., and Erin E. Noste. "Future Biological and Chemical Weapons." Edited by Gregory R. Ciottone, *Ciottone's Disaster Medicine*, U.S. National Library of Medicine, 2016, pmc.ncbi.nlm.nih.gov/articles/PMC7152330/.

Frischknecht, Friedrich. "The History of Biological Warfare. Human Experimentation, Modern Nightmares and Lone Madmen in the Twentieth Century." *EMBO Reports*, U.S. National Library of Medicine, June 2003, pmc.ncbi.nlm.nih.gov/articles/PMC1326439/.

"A History of Biological Weapons." *PBS*, Public Broadcasting Service, www.pbs.org/wgbh/americanexperience/features/weapon-timeline/. Accessed 4 Jan. 2025.

IHL, ihl-databases.icrc.org/en/ihl-treaties/cwc-1993. Accessed 4 Jan. 2025.

UN, documents.un.org/doc/undoc/gen/n04/328/43/pdf/n0432843.pdf?OpenElement=. Accessed 5 Jan. 2025.

"United Nations, Main Body, Main Organs, General Assembly." *United Nations*, United Nations, www.un.org/en/ga/first/. Accessed 4 Jan. 2025.

"What Is a Chemical Weapon?" *OPCW*, www.opcw.org/our-work/what-chemical-weapon. Accessed 4 Jan. 2025.