North Atlantic Treaty Organization (NATO)

Chair Letter

DEAR DELEGATES,

Welcome to the North Atlantic Treaty Organization (NATO) at CNYMUN 2026! As tensions increase internationally, diplomacy and cooperation are very important skills, possibly now more than ever. We look forward to seeing a productive and thoughtful conference with quality discussion about these greatly relevant modern issues that impact the global sphere. Chairing the North Atlantic Treaty Organization this year will be Yutaro Hirabayashi and Alia Bou Aram.

ABOUT THE CHAIRS:

Yutaro is a senior at Fayetteville-Manlius High School. This is his third year in MUN, and is looking forward to chairing for the first time. Outside of MUN Yutaro spends most of his time in his room playing electric guitar, only occasionally exiting to hit a chest day at the gym. Yutaro also types 217 words per minute on monkeytype and likes to build keyboards, currently owning 5.

Alia is a sophomore at Fayetteville-Manlius High School. This is her third year in MUN and she is especially excited for her first time chairing. Outside of MUN, Alia loves playing bass and collecting trinkets. When not studying or listening to music, she can often be found playing video games, practicing her tennis serve, or annoying her older brother.

ABOUT THE COMMITTEE:

The North Atlantic Treaty Organization (NATO) is a military and political alliance formed in 1949 in the early Cold War years to provide collective security, deterring Soviet and communist expansion, as well as countering nationalist militarism in post-World War II Europe. It was also intended to initially offer large-scale economic support to a struggling Europe.[1] With 32 member nations, NATO currently targets efforts towards safeguarding state freedom and security through both political consultation and military cooperation.[2] Today, the alliance undertakes a broad array of responsibilities, from collective defense under Article 5 to crisis management, counter-terrorism, and support for war zones.[3] In addition, NATO maintains partnerships and observer-like arrangements with multiple nonmember countries through frameworks like the Partnership for Peace, currently cooperating with 35 nonmember partners. Currently, alongside its partnerships, NATO makes efforts towards stabilizing vulnerable regions, both in and outside of member states, through capacity building missions, particularly concerning civilian freedoms and preventing illegal trafficking.[4]

Your topics for the North Atlantic Treaty Organization at CNYMUN 2026 will be:

1. Countering Terrorism and Hybrid Warfare
2. Securing CBRN Materials

ABOUT THE CONFERENCE:

Following CNYMUN tradition, the debate will be conducted in Harvard style, meaning delegates will not be allowed to use pre-written clauses and/or resolutions during the committee. Doing so will make a delegate ineligible for awards.

To be eligible for awards, delegates must submit a 1-2 page position paper via email that addresses both topics before the start of the conference. Position papers should outline the stance of your delegation and display an understanding of the topics, demonstrating research and knowledge of your organization's goals. When deciding on awards, the chairs will look favorably upon delegates who have put significant effort towards research/preparation, collaborate with other delegates during committee sessions, stay within their nation's policies, and get their voice heard without being overbearing.

Furthermore, CNYMUN has implemented a tiered structure of committees to ensure similar experience levels for all committee members. NATO is designated as an **advanced** committee, and we would like the debate to reflect that. In turn, the 'Best New Delegate' award will not be offered to any delegates in this committee.

[1]"North Atlantic Treaty Organization (NATO), 1949." *Milestones in the History of U.S. Foreign Relations — Office of the Historian*, U.S. Department of State, https://history.state.gov/milestones/1945-1952/nato.
[2]"Topic: NATO member countries." *NATO*, 11 March 2024, https://www.nato.int/cps/en/natohq/topics_52044.htm.
[3]"Topic: NATO operations and missions." *NATO*, 30 July 2025, https://www.nato.int/cps/en/natohq/topics_52060.htm.
[4]ibid.

The special features of mini crisis and double delegation will be used throughout the committee.

Additionally, note that for award purposes, there will be no bias for or against members and observer delegates.

Please share position papers before the conference begins. Our emails are listed below for you to contact your chairs about any research, position papers, committee inquiries, or other questions. We also encourage you to scan our lengthy delegate preparation resources and award structure on www.cnymun.org. We wish you luck and look forward to what CNYMUN 2026 will bring

Yutaro Hirabayashi
26yhirabayashi@fmschools.org

Alia Bou Aram
28abouaram@fmschools.org

TOPIC 1: COUNTERING TERRORISM AND HYBRID WARFARE

In the 21st century as cyber threats and nonstate actors grow more powerful, hybrid warfare and terrorism have become increasingly prevalent issues for the member states of NATO. Hybrid warfare is a method of warfare in which unconventional, non-militant methods such as disinformation campaigns and economic attacks are combined with traditional military force, and can be utilized by both state and non-state actors. Some common non-militant tactics include the use of propaganda, deception, sabotage, disinformation, and economic pressure, including sanctions and tariffs.

The use of hybrid warfare has multiple advantages for extremist groups and other rogue actors compared to traditional militant warfare. One significant advantage of hybrid warfare is that it often occurs in a grey zone under the threshold of traditional warfare, and allows nations to deny involvement in a conflict and avoid responsibility whilst advancing their objectives. Hybrid warfare also allows for important decision-makers and the public to be targeted through the globalized and connected media due to more recent advancements of information technologies. During the U.S presidential election in 2016, Russia was able to interfere with public opinion by spreading misinformation through social media and hacking political party servers such as the Democratic National Committee, while Russian officials including Putin consistently publicly denied any involvement.[5]

Terrorism is another threat to the security of NATO states that has endured through the 21st century, continuing to endanger the lives of civilians and destabilizing regions. Modern terrorism continues to evolve both ideologically and organisationally, making eliminating these groups completely difficult for national governments and NATO.[6] For example, ISIS has a decentralized organisation system in which lone-actor supporters worldwide aid their operations, so supporters in other regions remain unaffected even

[5]"Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election." Justice.gov, 13 July 2018, www.justice.gov/archives/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election.
[6]NATO. "Countering Terrorism." NATO, 25 July 2024, www.nato.int/cps/en/natohq/topics_77646.htm.

when leaders in Syria or Iraq are targeted. Terrorism is often carried out due to strong ideological, religious, or political beliefs, making groups resilient even after enduring losses or setbacks. Extremist groups such as ISIS and Al Qaeda for example still exist and operate today despite the significant military defeats they have faced, as their followers deeply resonate with their ideologies.
Together, hybrid warfare and terrorism directly counteract NATO's purpose to safeguard the freedom and security of all its members.

Hybrid warfare and terrorism take advantage of vulnerabilities that are especially concerning for NATO and its member states. Hybrid warfare and terrorist attacks are most effective against states with economic instability, political instability, or social division. Many NATO member states have fairly significant public debt, resulting in potential economic vulnerability. Italy, Greece, and the United States, for example, all have a debt-to-GDP ratio above 100, meaning that their national debt is greater than their entire annual economic output[7]. Hybrid warfare attacks also aim to undermine the legitimacy of state governments, causing distrust between governments and their people. A prominent recent example of this is when the Russian government utilized emerging technologies such as AI to create misleading deepfake videos of American candidates in the 2024 U.S. presidential election.[8] Other methods of spreading disinformation including false news stories and social media posts were also used in an attempt to undermine trust in U.S. elections. China and Russia have also increasingly used misinformation campaigns to push narratives in their favor. Chinese and Russian misinformation campaigns synchronise their content to have aligning content around major events, such as the Russian invasion of Ukraine. Media from both nations blamed the West for the escalation of the conflict. Unconventional methods such as Chinese "Spamouflage" (Dragonbridge) campaigns, in which sources of disinformation pose as human rights organisations, have been used in attempts to seem like reliable sources of information.[9] Weaker governments that are less trusted by their populations may be unable to effectively respond to coordinated hybrid warfare attacks, resulting in their populations being vulnerable. Populations of weaker governments often rely on weak or partisan media, which are easier targets of misinformation campaigns.[10] States with economies largely dependent on a single export market, specific suppliers, or foreign investment are also vulnerable. Some Southeastern NATO members also have weak foreign direct investment (FDI) security screening, which are laws and regulations that allow for governments to assess, and if necessary, prevent foreign investments that may threaten national security. An attempt made by an enemy power to buy critical infrastructure, ports, or energy companies for example would be prevented by FDI screening.[11] Particularly nations of Albania, North Macedonia, and Montenegro have no formal FDI screening laws in place or are still in the process of adopting them.

Although many NATO member states in Western Europe and North America are relatively stable, Turkey and Albania in particular have higher Fragile States Index scores; Fragile States Index (FSI) scores are determined by the Fund for Peace and assess nations based on factors including security, economic decline, and public services, and higher FSI scores indicate greater fragility.[12]

Hybrid warfare and terrorism are not issues that arose overnight, but rather issues that have developed from significant events reshaping the priorities of NATO. An early example of modern Hybrid warfare is the conflict between Israel and Hezbollah in 2006, in which a non-state actor utilized both conventional

[7] Roytburg, Eva. "The U.S. Is Joining Europe's Debt Club—Trump's 'Big Beautiful Bill' Could Fuel $38 Trillion Tab, Bigger than Italy or Greece by GDP Share." *Fortune.com*, 2025, fortune.com/2025/10/28/how-bad-is-debt-us-europe-italy-greece-crisis-gdp-big-beautiful-bill-trump/. Accessed 1 Nov. 2025.
[8] Klepper, David. "Russian and Iranian Groups Sanctioned over U.S. Election Disinformation." PBS News, 31 Dec. 2024, www.pbs.org/newshour/world/russian-and-iranian-groups-sanctioned-over-u-s-election-disinformation.
[9] "Hybrid Storm Rising: Russia and China's Axis against Democracy." Www.epc.eu, 2025, www.epc.eu/publication/Hybrid-storm-rising-Russia-and-Chinas-axis-against-democracy-64b158/.
[10] "Hybrid Threats, Vulnerable Order." CIDOB, 2022, www.cidob.org/en/publications/hybrid-threats-vulnerable-order.
[11] "Investment Screening." Policy.trade.ec.europa.eu, policy.trade.ec.europa.eu/enforcement-and-protection/investment-screening_en.
[12] The Fund for Peace. "Fragile States Index." *Fragilestatesindex.org*, 2023, fragilestatesindex.org/.

and unconventional means of warfare. Hezbollah used a combination of the media and social media to influence public perception of them, portraying them as the defenders of Lebanon. Guerilla warfare tactics were also used by Hezbollah, such as digging an extensive tunnel network under the border with Israel, and using hit-and-run attacks against Israeli forces, taking advantage of Lebanon's complex terrain. Another instance of the use of hybrid warfare is the "little green men", or masked and unmarked soldiers who were an effective form of hybrid warfare utilized by The Russian Federation during the conflict between Russia and Ukraine prior to the occupation of Crimea in 2014. These soldiers were armed normally, but remained always masked and wore unmarked uniforms. Between February and March 2014, the unmarked soldiers occupied and blockaded Simferopol International Airport, many of Ukraine's military bases in Crimea, and the Supreme Council of Crimea, all while the President of The Russian Federation Vladimir Putin continued to deny any Russian involvement in Ukraine.

NATO has taken a multitude of initiatives in response to the evolving threat of hybrid warfare and terrorism. Significant actions taken by NATO include the NATO Defence College Forum Paper, an analytical document first adopted in 2015, which called for actions such as the strengthening of cyber and energy resilience, increasing capabilities for responding to hybrid threats rapidly, enhancing counter-disinformation; and the Wales Summit Declaration, in 2014, in which NATO stated explicit commitment to ensure NATO "is able to effectively address the specific challenges posed by hybrid warfare threats, where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design."[13]

Regarding hybrid warfare, On 14 May 2008 NATO established the Cooperative Cyber Defence Centre of Excellence following the cyber attacks on Estonia in spring of 2007. The cyberattacks on Estonia were primarily Distributed Denial-of-Service (DDoS) attacks, which flooded networks making services such as banking, media, and government websites. [14]The cyberattacks on Estonia demonstrate how nations such as Estonia with infrastructures largely dependent on digital technologies are more vulnerable to cyber attacks. More recently, NATO and the European Union launched the Hybrid Threats Centre of Excellence in Helsinki Finland to coordinate responses to disinformation and cyberattacks. Furthermore, NATO formally recognized cyber defence as a core part of their collective security at the Warsaw Summit in 2016.

Following the terrorist attacks on the USA on September 11, 2001, NATO first invoked article 5 which states that an armed attack against one member of NATO would be seen as an attack against all members of NATO and will assist the ally that had been attacked. From mid-October 2001 to mid-May 2002, NATO launched its first anti-terror operation including seven NATO AWACS radar aircraft to help patrol the skies over the United States. Operation Active Endeavour was a NATO maritime mission from 2001 to 2016 which had the goal of detecting and deterring potential terrorist related activity by patrolling the Eastern Mediterranean Sea. In February of 2018 NATO launched mission Iraq to strengthen security forces in Iraq, ensuring they are able to fight against terrorism, prevent the return of ISIS, and to stabilize the country.

Advancements in technology have further amplified the magnitude of hybrid threats and terrorist attacks. Newer developments such as social media and deepfakes can be utilized to spread disinformation and weaken a population's trust in their governments. Deepfakes are images or videos generated by an artificial intelligence with the goal of creating media realistically portraying people or events, but in a narrative beneficial to the creator and are often used to spread disinformation. A convincing deepfake video of a state leader can be utilized to manipulate public opinion regarding them or influence elections. Cyberattacks can target critical infrastructures such as energy grids and transportation services for a relatively low cost, as well as allowing the attackers to claim to be not involved. NATO's

[13] NATO. "Wales Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales." NATO, 2014, www.nato.int/cps/en/natohq/official_texts_112964.htm.

[14]Ottis, Rain. Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective. 2008.

secretary-general Jens Stoltenberg, stated "Cyber-attacks can be as damaging as conventional attacks. A single attack can inflict billions of dollars' worth of damage to our economies".[15] The exploitation of encrypted messaging apps and online forums by terrorists for recruitment and coordination purposes has grown as encryption became more integrated into online messaging apps and mobile electronics. Many commonly used messaging apps such as Telegram and Whatsapp now offer end-to-end encryption, making it harder for authorities to detect communications between terrorists. A common method of encryption used by these messaging apps is symmetric encryption, in which a 256-bit key is used to encrypt and decrypt messages. There are 2^256 possible keys and is considered to be impossible to break, even with modern supercomputers.[16]

Advancements in technology may potentially empower NATO to better respond to hybrid threats and terrorism as well. Allied Command Transformation of NATO continues to develop implementation of AI into military operations, education, and capability development. NATO ACT states that reliable information is a strategic resource essential for effectively functioning AI, and works to improve data management across NATO.

Although many initiatives have been taken by NATO to combat hybrid warfare and terrorism, many constraints limit their effectiveness. NATO's commitment to raising available defence and security-related funds to 5% of gross domestic product (GDP) of nations by 2035 was adopted as NATO recognized the growing need to strengthen security, especially in response to the growing security threats of Russia and terrorism. However, the commitment places a significant financial burden on NATO states, particularly those with high public debt or inflationary pressures. Another element that may limit NATO's ability to respond to hybrid warfare and terrorism is the existing political fragmentation within NATO. The primary threat for Eastern European NATO member states is Russia, while West European and North American members of NATO have placed more attention on other global challenges, such as China. The military budgets of member states also vary significantly, causing states such as the U.S. and Poland that spend more on their militaries to feel a greater financial burden in supporting NATO.[17] In June of 2025 NATO set a goal of allocating 5% of GDP to cybersecurity and infrastructure investments, as well as for 3.5% of GDP to be allocated to military and defence by 2035. However, only 3 NATO members, Poland, Lithuania, and Latvia have currently met this goal of 3.5% GDP allocation toward defence.[18]

Delegates must recognize the political and strategic tensions within NATO that could complicate a synchronized response to a hybrid threat or terrorist attack resulting from different members' national priorities. Delegates must also consider the potential risks of newly developing technologies, such as AI, social media, drones, and encrypted communication services that have the potential to be exploited if not regulated and monitored properly.

[15] NATO. "Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London." *NATO*, 19 May 2019, www.nato.int/cps/en/natohq/opinions_166039.htm.
[16]Evans, Donald, et al. "FIPS 197 Federal Information Processing Standards Publication Advanced Encryption Standard (AES)." Advanced Encryption Standard (AES), 26 Nov. 2001, nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf, https://doi.org/10.6028/NIST.FIPS.197-upd1.

[17]North Atlantic Treaty Organization. Defence Expenditure of NATO Countries (2014–2023), NATO Communications and Information Agency, 7 July 2023, https://www.nato.int/nato_static_fl2014/assets/pdf/2023/7/pdf/230707-def-exp-2023-en.pdf
[18]NATO. "Information on Defence Expenditures." NATO, 3 Apr. 2025, www.nato.int/cps/en/natohq/topics_49198.htm.

QUESTIONS TO CONSIDER

1. How can NATO improve early detection and attribution of hybrid attacks, especially those exploiting AI, deepfakes, and encrypted communication platforms?
2. How can NATO member states better coordinate intelligence and cyber defence while maintaining national sovereignty?
3. How can NATO support vulnerable member states in developing policies to prevent foreign influence via economic or investment channels?

HELPFUL SOURCES:

"Countering terrorism"
https://www.nato.int/cps/en/natohq/topics_77646.htm

"Algorithmic invasions: How information warfare threatens NATO's eastern flank"
https://www.nato.int/docu/review/articles/2025/02/07/algorithmic-invasions-how-information-warfare-threatens-nato-s-eastern-flank/index.html

"Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote"
https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

TOPIC 2: SECURING CBRN MATERIALS

The securement of CBRN (Chemical, Biological, Radiological, Nuclear) materials has become a global priority since the beginning of the 20th century, after the usage of chemical and nuclear weapons in both World Wars, as well as the Cold War arms race. This has led to the development of institutions equipped with counter measures such as the Non-Proliferation Treaty (NPT) and the Chemical Weapons Convention (CWC), but despite this, modern challenges such as terrorism, weapon trafficking, and a lack of transparency continue to threaten global security. Due to a current rise in dual-use technologies, which are any scientific research advancements or developments that could be used for both civilian or military developments, and increasing geopolitical tensions, instability further complicates securement efforts.

The securement of CBRN (Chemical, Biological, Radiological, and Nuclear) materials has been a global security concern since the early 20th century. During World War I, the introduction of chemical weapons such as chlorine, phosgene, and mustard gas marked a new era of warfare, resulting in more than one million casualties globally.[19] Almost immediately following their usage in WWI, they were banned under the Geneva Protocol. This was not, however, the only instance of the usage or development of these kinds of weapons. In east Asia during the year 1936, Japan formed Unit 731 in Manchuria, which was a site for developing biological weapons using facilities that studied pathogens, drugs, and other natural phenomena. While it was promptly shut down after the end of World War II in 1945, it was later discovered by the Soviets with over 6,000 containers producing biological and chemical agents.[20]

Nuclear weapons, in contrast to chemical and biological weapons, have only been used once throughout history despite being stockpiled across the late 20th century. In 1945, Hiroshima and Nagasaki Japan, were bombed by United States' forces,

[19] "Chemical Weapons – UNODA." *United Nations Office for Disarmament Affairs*, https://disarmament.unoda.org/wmd/chemical/.
[20] Beckham, Haddie. "Unit 731 Map Found by the Soviet Union." *Pacific Atrocities Education*, 1 July 2020, https://www.pacificatrocities.org/blog/unit-731-map-found-by-the-soviet-union.

causing over 200,000 civilian deaths. The impacts of these two nuclear weapons did not stop at immediate deaths, but also led to increased risks of cancer development, most notably leukemia, which the Radiation Effects Research Foundation attributed to 46% of survivors.[21] The development of these nuclear weapons created what is known as the Nuclear Arms Race between the Soviet Union and the United States, which led to the amassment of tens of thousands of nuclear weapons between the end of WWII in 1945 and the dissolution of the Soviet Union in 1991.[22] At the same time, during the Vietnam War between 1955–1975, the United States military heavily used the herbicide Agent Orange to clear out paths in the forests. Over 11 million gallons of this herbicide were sprayed across approximately 20 million acres of Vietnamese land, as well as carried over into surrounding nations such as Cambodia. The repetitive usage of this chemical led to not only the development of lethal diseases, but also genetic birth defects. These genetic altercations and the presence of the chemical itself still affect regions of Vietnam, particularly the South.[23] For the past decades because of this, tensions between the United States and Vietnam have been high, even impacting trade abilities between the two regions, particularly because of the United States' repeated refusal to accept responsibility for the aftermath of Agent Orange. In recent years, the USA has taken some accountability, giving around 400 million dollars to the Vietnamese government.[24]

The Biological Weapons Convention (BWC) was opened for signatures in 1972 and entered into force in 1975 to prevent the development, stockpiling, and transfer of biological agents and weapons. Currently, the BWC has 187 member states as a legally binding treaty. Throughout almost the entirety of the 20th century, well past the signing of the BWC, from the 1920s to 1992, the Soviet Union ran a biological weapon program that weaponised diseases, such as smallpox, long after they stopped being naturally occurring. This Soviet Union Biopreparat developed, tested, and stockpiled biological weapons for the longest in the 20th century, until its prompt closure with the dissolution of the USSR.[25]

This problem did not stop at the end of the 20th century, with chemical weapons being seen repeatedly in the past two decades. In 2013, the Syrian Regime launched a chemical attack on the two Ghoutas at night, causing 1,144 deaths, 1,119 of them being civilians[26]. The attacks took an additional toll on its 5,935 survivors through recurring respiratory issues, further noting that nations continue to use these weapons even decades after banning them[27]. As an immediate aftereffect of Syria's chemical weapon usage, there had been threats of counter attacks made by the United States, United Kingdom, and France, until promises were made to slowly deplete the production.[28] In 2023, Israel's usage of white phosphorus in Gaza and Lebanon following October 7th were noted, since the chemical is known for causing burns and being used for fires and signaling. Israel has received no international consequences for this, which can be attributed to the fact that white phosphorus is not inherently considered a weapon.[29] As of 2025, chemical weapons have been brought into accusations against Russia after Dutch and

[21] Listwa, Dan. "Hiroshima and Nagasaki: The Long Term Health Effects | K=1 Project." *K=1 Project*, https://k1project.columbia.edu/news/hiroshima-and-nagasaki.
[22] "Timeline: U.S.-Russia Nuclear Arms Control." *Council on Foreign Relations*, https://www.cfr.org/timeline/us-russia-nuclear-arms-control
[23] "Agent Orange Effects & Symptoms." *Cleveland Clinic*, 10 February 2023, https://my.clevelandclinic.org/health/symptoms/24689-agent-orange-effects.
[24] Kumar, Ashish. "Addressing the Harmful Legacy of Agent Orange in Vietnam." *United States Institute of Peace*, 27 January 2022, https://www.usip.org/publications/2022/01/addressing-harmful-legacy-agent-orange-vietnam.
[25] Tiessan, Anna-Marie-Louise. "Biopreparat: The Soviet biological weapons programme." *University of Kent*, 16 March 2022, https://research.kent.ac.uk/kcwa/biopreparat-the-soviet-biological-weapons-programme/.
[26] Ashraph, Sareta. "Nine Years since Ghouta: Chemical Weapons in Syria." *Www.ushmm.org*, 22 Aug. 2022, www.ushmm.org/genocide-prevention/blog/nine-years-since-ghouta-chemical-weapons-in-syria.
[27] Alsaleh, Osama I., et al. "Acute Health Effects and Outcome Following Sarin Gas Attacks in Khan Shaykhun, Syria." *Cureus*, Feb. 2022, https://doi.org/10.7759/cureus.22188.
[28] Syrian Network for Human RIghts. "The 10th Anniversary of Two Ghoutas Attack: The Largest Chemical Weapons Attack by the Syrian Regime on Syrian Citizens." *reliefweb*, 20 August 2023, https://reliefweb.int/report/syrian-arab-republic/10th-anniversary-two-ghoutas-attack-largest-chemical-weapons-attack-syrian-regime-syrian-citizens-enar.
[29] "Israel: White Phosphorus Used in Gaza, Lebanon." *Human Rights Watch*, 12 October 2023, https://www.hrw.org/news/2023/10/12/israel-white-phosphorus-used-gaza-lebanon.

German officials claimed that the weapons had been used against Ukrainian civilians on the war front, specifically a choking agent that was first used by the Germans in WWI. Because of this, Russia has faced sanctions from international communities and has been removed from councils such as the Executive Council of the OPCW.[30]

While frequently used by government bodies and during conflicts, the usage of CBRN materials by terrorist organizations and non-state actors has become an increasingly prominent issue. In 1995, a Japanese doomsday cult used chemical weapons in the Sarin subway, killing 13 people and injuring well over 5,000.[31] In the United States as well, closely following the events of 9/11, letters laced with anthrax were sent by terrorist groups, killing 5 Americans and sickening 17 more.[32] Attacks such as these raise concerns that international regulations will not squash the issue, as even with treaties being enacted and security of dangerous materials being more efficient, there is still evidence of black markets and unauthorized transfers.

Modern efforts, including the establishment of treaties like the Non-Proliferation Treaty (NPT), the Chemical Weapons Convention (CWC), and the BWC, have attempted to prevent the spread and use of these weapons. However, loopholes in enforcement, limited verification capabilities, and a lack of transparency among certain states continue to pose challenges, such as how the NPT's language regarding nuclear material transfer doesn't entirely prohibit it in Article 3.2, or how the BWC doesn't have an international body to enforce it.[33]

Today, the securement of CBRN materials faces unique challenges driven by technological advancement and geopolitical instability, making most CBRN materials dual-use technologies. Rogue states, particularly concerning North Korea, China, Russia, Syria, and Iran, seek chemical or nuclear capabilities as deterrence strategies, while terrorist organizations and non-state actors exploit the accessibility of dual-use technologies.[34]

Ongoing research and innovations in biotechnology and synthetic biology present particular risks as well, as research intended for medical or agricultural purposes can be repurposed into biological weapons, hindering medical advancement capabilities. Additionally, fragile conflict zones, such as Yemen and the DRC that have long histories of human rights abuse and weak governments, lack the infrastructure needed to enforce international treaties, leading to persistent violations. The responses tend to involve sanctions and investigations, but almost always end in stalemates because of a lack of evidence on the accusation and the internal nature of the conflicts.[35] With the rise of cyber warfare, concerns have extended to the potential sabotage of nuclear power plants or radiological material theft. There's also a risk of discovery and abuse of orphaned research facilities, which has been seen in past conflicts with the theft of research to illegally sell. The Goiânia incident in Brazil for example, when abandoned capsules of cesium-137 were discovered and sold, contaminating the entire city in just days because these abandoned materials were not properly disposed of.[36]

Although monitoring mechanisms and international treaties exist, enforcement remains inconsistent due to political tensions and resource limitations. Therefore, the balance between scientific progress, such as the development of vaccines and treatments

[30] Deutsch, Anthony, et al. "Russian use of chemical weapons against Ukraine 'widespread', Dutch defence minister says." *Reuters*, 4 July 2025, https://www.reuters.com/world/europe/russian-use-chemical-weapons-against-ukraine-widespread-dutch-defence-minister-2025-07-04/.

[31] "Aum Shinrikyo: The Japanese cult behind the Tokyo Sarin attack." *BBC*, 6 July 2018, https://www.bbc.com/news/world-asia-35975069.

[32] "Amerithrax or Anthrax Investigation — FBI." *FBI*, https://www.fbi.gov/history/famous-cases/amerithrax-or-anthrax-investigation.

[33] Gonzalez, Lulu Victoria. "AUKUS and nuclear nonproliferation: allies or enemies?" *Global Affairs*, 3 January 2023, https://en.unav.edu/web/global-affairs/el-aukus-y-la-no-proliferacion-nuclear-aliados-o-enemigos#:~:text=At%20present%2C%20this%20loophole%20is,this%20case%20of%20the%20NPT.

[34] Tucker, Jonathan B. "The Current Bioweapons Threat - PMC." *PubMed Central*, https://pmc.ncbi.nlm.nih.gov/articles/PMC7123542/.

[35] "Human Rights Violations in Conflict Zones: What Can Be Done?" *PCRF*, https://www.pcrf.net/information-you-should-know/item-1718652928.html.

[36] "The Goiânia incident, the semiotics of danger, and the next 10,000 years." *PubMed*, https://pubmed.ncbi.nlm.nih.gov/37535035/.

in the medical field, and security oversight remains a pressing challenge for the international community.

Delegates should carefully consider the regional political tensions coinciding with this topic due to the nuanced history associated with these newer technologies. Delegates should also take note of the risks of sharing these materials within regions of weaker infrastructural capabilities due to the potential of monopolizing or exasperating the industry there. Delegates must focus on ameliorating infrastructures in vulnerable areas in order to encourage innovation without increasing the risks of these dual-use technologies.

QUESTIONS TO CONSIDER:

1. What security measures can be enforced to strengthen the enforcement of existing treaties such as the NPT, CWC, and BWC?
2. How can states and organizations respond to the CBRN threat posed by non-state actors?
3. What role can capacity-building and intelligence sharing play in preventing proliferation in fragile states?
4. Since CBRN materials offer potential advancements, how can CBRN research be managed without creating new threats or stalemating innovations?

HELPFUL SOURCES:

"Weapons of Mass Destruction"
https://disarmament.unoda.org/en/our-work/weapons-mass-destruction#:~:text=UNODA%20provides%20substantive%20support%20in,be%20deadly%20and%20highly%20contagious.

"CBRN Risk Mitigation and Security Governance Unit"
https://disarmament.unoda.org/en/our-work/weapons-mass-destruction#:~:text=UNODA%20provides%20substantive%20support%20in,be%20deadly%20and%20highly%20contagious.

"Future Bioterror and Biowarfare Threats for NATO's Armed Forces until 2030"
https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MCU-Journal/JAMS-vol-14-no-1/Future-Bioterror-and-Biowarfare-Threats/