AMPSMUN 2025

Disarmament and International Security Committee

DISEC

Table of Contents:

Letter From The Chairs

Dear Distinguished Delegates,

It is our distinct honor to welcome you to AMPSMUN 2025 as the Chairperson and Deputy Chairperson of the Disarmament and International Security Committee (DISEC). Together, we will address one of the most pressing security challenges of our time – the threat of nuclear weapons falling into the hands of non-state actors. We are confident that our deliberations will be both engaging and impactful.

The proliferation of nuclear weapons has always been a significant concern for the international community. However, the emerging threat of non-state actors acquiring nuclear capabilities
presents an unprecedented challenge to global security. Addressing this issue requires innovative solutions that transcend traditional state-centric approaches to nuclear security and non-proliferation.

To seasoned MUN participants, we promise thought-provoking debates that will challenge your diplomatic skills. For first-time delegates, we are here to guide you through this exciting journey. Remember, the true essence of Model UN lies not only in speaking but also in listening, negotiating, and working collaboratively to achieve consensus.

We encourage you to thoroughly research your country's stance, explore the complexities of nuclear security, and come prepared for substantive discussions. Your active participation and creative ideas will play a vital role in crafting comprehensive solutions to this critical global issue.

Best regards,
Manas Kankarej, Head Chair
Vansh Dhingra, Co Chair
DISEC AMPSMUN 2025

Committee Focus

The Disarmament and International Security Committee (DISEC) is the First Committee of the United Nations General Assembly and plays a pivotal role in addressing issues related to global peace and security. Established in 1945, DISEC was created in the aftermath of World War II with the primary goal of fostering international stability and preventing future conflicts.

The committee is tasked with dealing with a wide range of issues, including disarmament, the regulation of armaments, and addressing global challenges that pose threats to international peace and security.

As part of its mandate, DISEC provides a platform for member states to engage in dialogue and cooperation on pressing security issues, aiming to find multilateral solutions that uphold the principles of the United Nations Charter. The committee works closely with other bodies, such as the United Nations Disarmament Commission (UNDC) and the Geneva-based Conference on Disarmament (CD), to ensure coherence and collaboration in the global disarmament agenda.

DISEC's agenda covers an extensive array of topics, from conventional weapons and arms trade to nuclear disarmament and emerging threats posed by technological advancements in warfare. By addressing these critical issues, DISEC seeks to build trust among nations, reduce the risks of armed conflict, and promote a secure and peaceful international environment.

Its work is integral to the broader objectives of the United Nations, contributing to sustainable development and the protection of human rights through the prevention of violence and conflict

Background Topic

Agenda 1 : Challenges in nuclear nonproliferation: Tackling the threat of non-state actors gaining nuclear capabilities

The struggle against nuclear proliferation presents several fresh and urgent challenges in the modern era. Chief among these is the risk of nuclear materials falling into the hands of non-state actors—such as terrorist groups—that operate outside international legal norms, rendering traditional deterrence strategies far less effective. Worse still, there are numerous ways these groups might attempt to acquire nuclear capabilities, making the situation increasingly complex and serious.

One significant concern is the theft of nuclear materials from facilities housing everything from weapons-grade uranium to spent fuel. While security measures exist, they are not foolproof, leaving room for insider threats and external attacks. This is particularly concerning in politically unstable regions, where vulnerabilities are heightened. Recent incidents have underscored just how penetrable some sites remain, emphasizing the urgent need for stricter protective measures.Another alarming avenue is the black market. Following the dissolution of the Soviet Union, numerous cases of nuclear material trafficking came to light, exposing networks that remain active and have since become more sophisticated and harder to dismantle. Some of these operations involve organized crime, adding another layer of complexity to the challenge.

Perhaps the most frightening possibility is non-state actors constructing their own nuclear devices. While building a fully functional weapon requires significant expertise, creating a simpler device is not beyond reach. Technical knowledge is increasingly accessible online, and the proliferation of dual-use technologies—tools that serve both civilian and military purposes—makes it easier for determined groups to take dangerous steps.
Cybersecurity is another critical area of concern. As nuclear facilities rely more heavily on digital systems, they become vulnerable to cyberattacks. A successful hack could lead to stolen nuclear materials or, worse, a catastrophic accident. Cyber threats are particularly challenging because attackers can strike from anywhere, and identifying them is often difficult.

Civilian nuclear programs, typically aimed at energy production or research, also pose risks. The technology used in these programs can be exploited for malicious purposes. Non-state actors might infiltrate such programs or coerce insiders into cooperating. Balancing the peaceful use of nuclear technology with the need for robust security measures remains a major challenge for the international community.
What makes these threats even more challenging is their tendency to overlap. Non-state actors often employ multiple strategies simultaneously, complicating efforts to predict or prevent their actions. Addressing these risks requires a unified global response. Nations must share intelligence, collaborate on security initiatives, and invest in advanced technologies to stay ahead of these threats.

Key Issues

- **Technological Vulnerabilities:**

The increasing digitalization of operations in nuclear facilities has introduced a range of cybersecurity risks, making them potential targets for exploitation by malicious actors. Non-state actors, such as terrorist groups or criminal organizations, could exploit these vulnerabilities to gain unauthorized access to sensitive systems, potentially allowing them to steal nuclear materials, disrupt critical processes, or sabotage the facilities themselves. This risk is further compounded by the difficulty of tracing and countering cyberattacks, given the anonymity and global reach afforded by digital technologies. Enhanced cybersecurity measures and international collaboration are essential to mitigate these threats and safeguard nuclear infrastructure.

- **Material Security:**

Despite notable progress in enhancing nuclear security worldwide, significant gaps remain, particularly in regions marked by political instability or limited resources. Large quantities of weapons-grade nuclear material and radioactive substances continue to be inadequately secured in various locations, posing a substantial risk of theft or misuse. Insider threats, weak regulatory frameworks, and outdated security measures exacerbate these vulnerabilities, increasing the likelihood that such materials could fall into the hands of non-state actors. Strengthening global efforts to secure nuclear materials is crucial to prevent their diversion for malicious purposes.

- **Information Proliferation:**

The widespread accessibility of the internet has created new challenges in controlling the dissemination of information related to nuclear weapons and technologies. Technical knowledge, including the basics of nuclear weapons design and manufacturing, can now be accessed online, often with limited barriers. Although much of this information may be incomplete or inaccurate, it still provides enough guidance to encourage or assist individuals and groups in attempting to develop nuclear capabilities. The availability of this information underscores the need for stronger international mechanisms to monitor and control the spread of sensitive knowledge while promoting education and awareness about the risks associated with its misuse.

Major Parties Involved

United States:
Leads the globe in nuclear security, providing technical assistance and funding for security improvements around the world. The U.S. has the largest budget for nuclear security and has very extensive programs for the detection and prevention of nuclear trafficking.

Russian Federation:
Has the world's largest nuclear arsenal and large quantities of civilian nuclear materials. Russia's cooperation is essential to global nuclear security efforts, especially in securing Soviet-era nuclear materials.

International Atomic Energy Agency:
The global atomic guardian on technical guidance for security recommendations and verification. The role of the IAEA in preventing the acquisition of nuclear materials by non-state actors has considerably expanded since 9/11.

European Union:
Contributes a great deal to global nuclear security, with funding, research, and coordination of member state security initiatives. The nuclear security framework of the EU acts as a model for regional cooperation.

Non-State Actors:
These are terrorist organizations, criminal networks, and black market operators. Their motives also range from financial to ideological, making it difficult to prevent such incidents.

Past Attempts To Solve The Issue

The international community has developed a comprehensive framework of treaties, resolutions, and initiatives to address the challenges of nuclear proliferation and security, particularly focusing on non-state actors in recent decades:

1. Nuclear Non-Proliferation Treaty (NPT)

The NPT, which entered into force in 1970, remains the cornerstone of the global nuclear nonproliferation regime. The treaty rests on three fundamental pillars: non-proliferation, disarmament, and peaceful use of nuclear energy. Primarily, it is meant to operate at the level of states.
Proliferation, the NPT has provided important building blocks for nuclear security in preventing the diversion of nuclear materials to non-state actors. In this connection, the NPT obliges non-nuclear weapons states to accept comprehensive IAEA safeguards on all their nuclear materials and facilities. These establish a verification regime preventing diversion of nuclear materials. Regular Review
Conferences held every five years allow strengthening the implementation of the treaty and take stock of emerging challenges.

2. UN Security Council Resolution 1540 (2004)

UNSCR 1540 represents the first comprehensive international effort specifically targeting
non-state actor acquisition of weapons of mass destruction. The resolution imposes three main obligations on all UN member states:

- Prohibit support to non-state actors seeking WMDs
- Adopt and enforce effective laws prohibiting WMD activities by non-state actors
- Implement domestic controls to prevent WMD proliferation

The resolution also provided for the establishment of a 1540 Committee for monitoring implementation and providing technical assistance to states. Regular reviews are conducted by the Committee, which helps to identify gaps in national efforts at implementation. Its mandate has been extended several times, reflecting its relevance to the international security architecture.

3. Nuclear Security Summit Process (2010-2016)

The Nuclear Security Summit process, which was initiated by U.S. President Barack Obama, was a series of world summits aimed at strengthening international cooperation on nuclear security. Four summits were held:

- Washington (2010): Established the basic framework for international cooperation
- Seoul (2012): Focused on radiological security and transportation
- The Hague (2014): Strengthened the international nuclear security architecture
- Washington (2016): Created action plans for key international organizations These summits produced concrete commitments by the participating states, including the

Past Attempts To Solve The Issue

Repatriating highly enriched uranium to research facilities
- Converting reactors to utilize low-enriched uranium
- Enhanced port and border security
- Providing Centers of Excellence for nuclear security training
- Legislating new controls to secure radiological sources

4. Global Initiative to Combat Nuclear Terrorism (GICNT)

Founded in 2006 by Russia and the United States, today GICNT has expanded to 89 partner nations and six observer organizations. The initiative works on:
- Strengthening Global Capacity to Prevent, Detect, and Respond to Nuclear Terrorism
- Bringing together police, intelligence, technical, and other experts
- Organizing workshops, exercises, and conferences to share best practices
- Developing guidelines on nuclear detection, nuclear forensics, and response

5. Convention on the Physical Protection of Nuclear Material (CPPNM)

The CPPNM, adopted in 1979 and amended in 2005, establishes legally binding standards for physical protection of nuclear materials. The amended convention:
- Applies protection requirements to domestic use, storage, and transport
- Criminalizes nuclear smuggling and sabotage
- Expands international cooperation mechanisms
- Forces states to protect nuclear facilities against sabotage

6. Proliferation Security Initiative (PSI)

Launched in 2003, PSI is an informal international partnership that aims to interdict traffic in WMD-related materials. The initiative
- Promotes information sharing among participating states
- Harmonizes procedures for intercepting suspicious shipments
- Conducts joint exercises to improve interdiction capabilities
- Develops best practices for detecting and interdicting proliferation.

7. IAEA Code of Conduct on the Safety and Security of Radioactive Sources

This non-binding instrument gives guidance on the following aspects:

- Establishing national registers of radioactive sources
- Establishing import/export controls
- Managing orphan sources
- Securing sources during the whole life cycle

Past Attempts To Solve The Issue

8. Regional Initiatives

A number of regional organizations have established their nuclear security initiatives, including the following:

- European Union: Chemical, Biological, Radiological and Nuclear Risk Mitigation Centres of Excellence
- Association of Southeast Asian Nations (ASEAN): Regional Convention on Counter Terrorism
- African Union: African Nuclear-Weapon-Free Zone Treaty (Pelindaba Treaty)

These different international actions create an intricate web of crossed-cutting initiatives and responsibilities, and while they have strengthened global nuclear security in numerous ways, challenges remain, especially in the following regards:

1. Universal participation
2. Maintaining political momentum
3. Ensuring consistent funding
4. Coordination between different initiatives
5. Dealing with emerging threats
6. Strengthening verification mechanisms

Focus Questions

1. How can the international community strengthen physical security at nuclear facilities while respecting national sovereignty?

2. What role can emerging technologies play in detecting and preventing nuclear material trafficking?

3. How can states improve cooperation in sharing intelligence about potential nuclear threats from non-state actors?

4.What measures can be implemented to prevent insider threats at nuclear facilities?

5. How can the international community address the challenge of nuclear security in regions with limited resources or infrastructure?

Background Topic

Agenda 2: Disinformation Campaigns and International Security: Addressing the Threat of State-Sponsored Fake News and Psychological Warfare:

Disinformation campaigns have emerged as one of the most pressing threats to international security in the 21st century. Unlike traditional warfare, information warfare operates within a gray zone between peace and conflict, making it particularly challenging to address using conventional security frameworks. The rapid development of digital technologies and the sophistication of modern disinformation campaigns have imposed unprecedented challenges on national security and international stability.

A particularly alarming aspect of this threat is state-sponsored disinformation targeting democratic processes. These campaigns manipulate public opinion, interfere with electoral procedures, and erode trust in institutions, particularly during critical political moments. The consequences can be profound, with long-lasting impacts on national sovereignty and international relations.

Social media platforms have become the primary battleground for information warfare. The speed of information dissemination, combined with algorithmic amplification, allows disinformation to spread faster than truth. State actors have developed elaborate structures, including automated accounts, troll farms, and coordinated inauthentic behavior, to maximize the reach and influence of their campaigns.

Adding another layer of complexity, artificial intelligence (AI) and deep fake technologies have introduced new dimensions to this threat. These advanced systems can create highly convincing fake videos, audio, and text, making it increasingly difficult for individuals and organizations to discern fact from fiction. Such capabilities have significant implications for diplomatic relations, crisis management, and conflict prevention.
Targeted disinformation campaigns also serve as tools of psychological warfare, enabling state and non-state actors to achieve strategic objectives with minimal resources.

These operations can exploit specific demographic groups, foster social division, undermine institutional trust, and propagate extremist ideologies.
The evolution of disinformation as a security threat can be traced through several key phases. During the Cold War, systematic propaganda campaigns were employed by both Eastern and Western blocs to shape global narratives and influence public opinion. With the advent of the internet in the 1990s, new avenues for information dissemination emerged, exponentially increasing the reach and impact of such campaigns.

The 2016 U.S. presidential election marked a watershed moment, exposing the vulnerability of social media to state-sponsored disinformation. This period brought heightened awareness to the global scale and complexity of the disinformation threat, leading to calls for more robust international measures to counteract its impact.

Key Issues

The landscape of disinformation campaigns and their implications for international security have changed dramatically over the past few years. Today, the information security environment is characterized by confluences of technological vulnerabilities and operational sophistication with emerging threats that are placing disinformation at the tip of the spear in respect to national concern around the globe.

Technological Vulnerabilities and Advances

With AI and deep fake technology, there has been a great revolution in creating and spreading false information. Advanced AI systems are now capable of generating highly convincing fake videos, images, and audio; on the other hand, with language models like GPT, false narratives can be created automatically. The increasing quality and ease of access to deep fake technology are going to make it increasingly hard for people to distinguish what's real and what's manipulated.
Social media platforms, through algorithmic promotion of content, often amplify sensational and divisive content, creating echo chambers that reinforce users' existing beliefs while limiting exposure to diverse perspectives. This becomes all the more problematic in light of the ability to micro-target demographics with tailored disinformation, whereby malicious actors can precisely influence vulnerable populations.

Operational Patterns

The disinformation campaigns have become more sophisticated, often forming part of a larger hybrid warfare strategy. State actors now routinely engage in cross-border operations through proxy
networks to mask the true creators of disinformation. The campaigns are usually combined with traditional military operations, cyber attacks, and economic pressure tactics to have the greatest impact on target nations.

New Challenges

One such area is that of critical infrastructure: mis- and disinformation campaigns have often zeroed in on false narratives about health systems, energy infrastructure, and financial markets to sow panic among the public and destabilize society. Democratic processes will be faced with yet another dimension of threats through complex voter suppression tactics, manipulation of political discourse, and creating false narratives around electoral integrity.

Major Parties Involved

- United States: The United States has taken significant steps to counter disinformation, primarily through the creation of organizations such as the Global Engagement Center. This body focuses on countering foreign propaganda and providing accurate information to combat the influence of state-sponsored disinformation campaigns. Additionally, the U.S. government collaborates with private organizations and international allies to address the growing threat of false narratives online.

- Russian Federation: Russia has been a key player in the proliferation of disinformation campaigns, utilizing sophisticated tools and dedicated information warfare units such as the Internet Research Agency. These units conduct large-scale, coordinated campaigns aimed at influencing public opinion, destabilizing democratic institutions, and spreading false narratives both domestically and internationally.

- People's Republic of China: China operates an extensive and highly organized network for narrative control. Through state media, cyber tools, and social media platforms, the Chinese government amplifies its preferred narratives while suppressing dissenting voices. Its global disinformation efforts are often tied to advancing geopolitical objectives, influencing foreign policies, and promoting its image on the world stage.

- European Union: The EU has emerged as a leader in combating disinformation through the development of comprehensive regulatory frameworks. These initiatives aim to hold online platforms accountable for the content they host, promote transparency in digital advertising, and reduce the spread of false information. Additionally, the EU invests in public awareness campaigns and collaborates with member states to tackle disinformation collectively.

- Big Technology Companies: Major technology companies such as Meta, Twitter, and Google play a critical role in addressing the spread of disinformation. They have implemented measures such as fact-checking, algorithmic adjustments, and content moderation policies to limit the reach of false information. However, these efforts remain under scrutiny due to concerns about their effectiveness and transparency.

- Atlantic Council's Digital Forensic Research Lab: This non-governmental organization conducts vital work in the analysis and research of disinformation campaigns. By tracking online manipulation, exposing coordinated inauthentic behavior, and developing tools for identifying disinformation, the lab provides critical insights and supports global efforts to counter the threat.

Past Attempts To Solve The Issue

The international community has undertaken various efforts to address the threat of disinformation campaigns and its consequences on international security:

- Efforts by the United Nations

The UN has identified disinformation as a threat and has taken some actions:

UN Strategy and Plan of Action on Hate Speech,
2019: Though this initiative specifically targets hate speech, it is highly interconnected with disinformation campaigns.
Verified Initiative (2020): Launched by the UN to counter COVID-19 misinformation, the website provides actual information to counter false narratives

- Regional Initiatives

1.Other regional organizations have developed their own initiatives toward the same objective:

2.European Union: Has implemented the Action Plan against Disinformation and the Code of Practice on Disinformation, whereby it engages tech companies in combating false information.

3.NATO: Established the Strategic Communications Centre of Excellence to develop strategies for countering disinformation

- Tech Company Efforts

Major tech platforms have responded with efforts to mitigate disinformation, including:

1.Content moderation policies: Facebook, Twitter, and YouTube have formulated policies on the removal or flagging of false information

2.Fact-checking partnerships: Collaborations with independent third-party fact-checkers to validate content and flag possibly false information1

- Civil Society and Academic Initiatives

Some of the NGOs and academia that have contributed towards solving disinformation include:

1.Atlantic Council's Digital Forensic Research Lab: Researches and analyzes disinformation campaigns.

2.First Draft: A not-for-profit organization that provides training and tools for journalists to fight misinformation.

These efforts notwithstanding, state-sponsored disinformation campaigns continue to present a huge challenge that requires more international cooperation and new creative solutions to chart this dynamic threat against global security.

Focus Questions

1. How can the international community develop comprehensive strategies to counter state-sponsored disinformation?

2. What legal frameworks can be created to address information warfare without compromising free speech?

3. How can emerging technologies like AI and deep fakes be regulated to prevent their misuse in disinformation campaigns?

4. What technological solutions can help distinguish between authentic and manipulated content?

5.How can societies build resilience against targeted psychological warfare?

6.What mechanisms can be developed to prevent social division caused by disinformation?

7. How can nations collaborate to detect and neutralize cross-border disinformation operations?

8.What role should social media platforms play in combating false narratives?

9. How can electoral systems be protected from disinformation campaigns that aim to manipulate public opinion?

10. What strategies can safeguard democratic institutions from information warfare?

11. How can critical infrastructure be protected from potential disinformation attacks?

12. What new forms of psychological warfare might emerge with advancing technology?

Recommended sources

Agenda 1 :

1.Nuclear Non-Proliferation Treaty (NPT)
2.UN Security Council Resolution 1540
3.Nuclear Security Summit Process (2010-2016)
4.Global Initiative to Combat Nuclear Terrorism (GICNT)
5.Convention on the Physical Protection of Nuclear Material (CPPNM)
6.Proliferation Security Initiative (PSI)
7.IAEA Code of Conduct on the Safety and Security of Radioactive Sources
8.Regional nuclear security initiatives (EU, ASEAN, African Union

Agenda 2 :

1."The Weaponization of Information: The Need for Cognitive Security" by RAND Corporation
2. "Information Warfare in the Age of Cyber Conflict" by Christopher Whyte and Brian Mazanec
3."LikeWar: The Weaponization of Social Media" by P.W. Singer and Emerson T. Brooking
4. "The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age" by Adam Segal
5. "Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics" by Yochai Benkler, Robert Faris, and Hal Roberts

Bibliography

Agenda 1 :

1.Bradshaw, S., & Howard, P. N. (2019). The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation. Oxford Internet Institute.

2.European Commission. (2018). Action Plan against Disinformation. Brussels: European Commission.

3.NATO Strategic Communications Centre of Excellence. (2019). Countering Information Influence Activities: A Handbook for Communicators. Riga: NATO StratCom COE.

4.Nimmo, B. (2015). Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It. Central European Policy Institute.

5.United Nations. (2019). United Nations Strategy and Plan of Action on Hate Speech. New York: United Nations.

6.Wardle, C., & Derakhshan, H. (2017). Information Disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe Report.

7.Woolley, S. C., & Howard, P. N. (Eds.). (2018). Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media. Oxford University Press.

8.Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Profile Books

Agenda 2 :

1.International Atomic Energy Agency (IAEA) publications

2.United Nations Office for Disarmament Affairs (UNODA) resources

3.Nuclear Threat Initiative (NTI) reports

4.Stockholm International Peace Research Institute (SIPRI) yearbooks

5.Arms Control Association fact sheets and reports

AMPSMUN

AL MAAREF PRIVATE SCHOOL