BULLSMUN III

Disarmament and International Security Committee

Topic I: Strengthening International Cooperation in Cybersecurity

Topic II: The Role of Non-State Armed Actors in Modern Conflict

Chair Introduction

Hey everyone! My name is Natalia Lima, and I am so excited to be your chair for BULLSMUN III. I'm a senior at USF, double majoring in Psychology and Integrated Public Relations & Advertising. While my majors may not directly scream "international affairs," my passion for global issues and Model UN runs deep. I started Model UN back in 8th grade, and I haven't stopped since.

Something about meeting new people, learning about real-world issues, and working to find solutions through debate and diplomacy has kept me engaged for all these years. I currently serve as the President of USF MUN, and I'm thrilled to be leading DISEC—my all-time favorite committee—this conference weekend.

I hope you enjoy reading this background guide and find it helpful as you dive into your research. I love both of the potential topics and can't wait to see the creative solutions and exciting debates you'll bring to the table. If you have any questions before the conference, feel free to reach out to me at natalia100@usf.edu. See you soon!

Committee Format

This committee will serve as a double-delegate General Assembly. Though delegates have been given two topics in this background guide, they should expect to only debate one topic over the course of BULLSMUN weekend. Delegates on the Speakers List will advocate for the topic of their choice at the beginning of the committee. The topic of debate will then be decided via a majority vote.

Committee Introduction

The Disarmament and International Security Committee, commonly known as DISEC or the First Committee of the United Nations General Assembly, serves as a central venue where Member States address evolving threats to international peace and security. As technological change redraws the boundaries of conflict, DISEC provides a diplomatic space where states can negotiate norms, form policies, and explore multilateral frameworks to manage emerging security challenges. Its focus is global issues and its authority is rooted in diplomacy and consensus-building among UN members.

Topic I: Strengthening International Cooperation in Cybersecurity

Introduction

Across the interconnected digital landscape of today, cyberattacks are no longer limited to petty crimes. They now include operations that can disrupt electricity grids, compromise elections, steal critical data, or threaten financial systems. Many such operations are tied to states either directly or through indirect support. The borderless nature of cyberspace complicates how the global community defines acceptable conduct. States and organizations often struggle not only with attributing attacks to the correct actor but also with holding identified perpetrators responsible for their actions. At the same time developing countries frequently confront challenges in building the technical and legal infrastructure needed to respond effectively. This convergence of threats, gaps, and challenges lies squarely within DISEC's mandate and creates an urgent need for immediate discussion and action.

Historical Analysis

In the early 2000s, as cyber incidents proliferated, their implications began receiving serious attention from international policymakers. The United Nations appointed a Group of Governmental Experts (GGE) to examine how traditional international law applies to cyberspace. The GGE's conclusions signaled a shift—cyber issues belonged on the international peace and security agenda, not just in the domain of criminal justice and commercial regulation.

As the decade progressed, states developed voluntary norms and confidence-building proposals intended to foster responsible behaviour in cyberspace. These initiatives included commitments to safeguard critical infrastructure, avoid involvement in cybercrime, and uphold human rights online. Although widely circulated and endorsed in principle, these norms lacked the force of law and left many questions unanswered about how they should be applied in practice.

Efforts to transform these voluntary commitments into binding international rules quickly ran into political and regional divisions. Major power blocs held divergent views on core issues like whether cyberspace required new treaties, or whether existing international law was adequate. In response, the UN created Open-Ended Working Groups (OEWG) to include more states in deliberations and expand ownership of the process. Over the years, these groups have issued reports recommending confidence-building measures, greater information sharing, and capacity-building programs to help states—especially developing ones—improve their defenses and responses to cyber threats.

While these diplomatic debates continued, other forces also shaped how the world thought about cyber conflict. Scholars and legal experts worked to clarify how international law applies to cyberspace. One of the most influential efforts was the *Tallinn Manual* series, which provides expert interpretations of rules governing issues like sovereignty and state responsibility in the context of cyber operations. Though not legally binding, these analyses have guided government policies and fueled academic debate.

At the same time, real-world cyber incidents—from ransomware attacks on infrastructure to espionage campaigns and electoral interference—were unfolding. These high-profile cases made the challenges feel urgent, sparking demands for greater clarity, transparency, and accountability. But they also exposed a central problem: attribution. Technical forensics can sometimes point to likely culprits, but proving responsibility in a way that is both credible and politically acceptable remains extremely difficult.

Past International Actions

In the UN system, experts and working groups on cybersecurity have agreed that international law applies to cyberspace and have suggested voluntary norms to guide state behavior.. While these efforts advance shared understanding, their non-binding nature limits enforcement and leaves room for disagreement.

On the academic and legal front, the *Tallinn Manual* has become an important reference. It analyzes how states behave in cyberspace and explains how existing laws apply to cyber operations. Because it is not an official treaty, however, it serves only as a guide rather than a set of enforceable rules.

Attribution—the process of figuring out who is behind a cyberattack—continues to develop. Governments, often with help from private companies, use tools like technical forensics, data tracing, and intelligence-sharing to build their cases. Sometimes they share their findings publicly, while other times they keep them classified for diplomatic or security reasons. Still, the technical and legal hurdles are so complex that creating firm, widely accepted attributions remains very difficult.

On the cybercrime front, the Budapest Convention on Cybercrime provides a legally binding framework for international cooperation. It helps countries work together on investigations and share evidence across borders. Although not every country has signed on, it remains a central tool for dealing with global cybercrime.

Recognizing that not all states have the same resources to respond to threats, international initiatives like the Global Forum on Cyber Expertise (GFCE) have stepped in. These programs support countries in creating cybersecurity strategies, building national Computer Emergency Response Teams (CERTs), updating their legal systems, and training technical experts. Building shared capacity is essential for making the global community more resilient and fair.

Taken together, these efforts form a patchwork of norms, legal guidance, technical practices, and capacity-building. Despite these advances, major gaps remain, leaving the global community with ongoing challenges.

Next Steps

Looking ahead, DISEC delegates can help move the discussion from broad ideas toward clearer commitments—especially where there is already wide agreement, such as protecting non-military infrastructure during peacetime. Starting with areas of consensus can build momentum while still respecting the concerns of individual states.

Delegates might also consider frameworks for cooperative attribution, which would allow countries to share information on cyber incidents and build trust. These systems would need to strike a balance between being open and protecting sensitive intelligence sources and methods.

Another key priority is capacity-building. DISEC could support programs that help states strengthen their own cyber defenses—through national response teams, updated laws and regulations, and training—while ensuring these efforts respect sovereignty and encourage local ownership.

The detailed legal analysis found in sources like the *Tallinn Manual* can also support international dialogue. It helps states clarify their responsibilities in cyberspace without requiring them to immediately negotiate new, highly technical treaties.

Finally, improving transparency and trust through confidence-building measures—such as incident notification systems or reliable communication channels—can reduce misunderstandings and encourage cooperation without being overly restrictive.

Together, these approaches give delegates a range of options to craft balanced, practical solutions, grounded in diplomacy, law, fairness, and collective security.

Questions to Consider

1. What policies and actions could support states—particularly developing ones—in building the technical, legal, and institutional capacity needed to uphold international cyber norms?
2. Which aspects of responsible state behaviour, such as protecting critical infrastructure, could realistically be elevated from voluntary norms to binding commitments?
3. What kind of attribution framework could enhance trust and accountability while safeguarding sensitive intelligence and avoiding escalation?
4. In what ways can interpretive tools like the Tallinn Manual inform consensus about state conduct in cyberspace without treaty obligations?
5. What measures would help reduce misperceptions and encourage transparency among states?
6. How should the international community differentiate responses to cyber operations carried out by non-state actors with state support versus those ordered directly by states?

Topic II: The Role of Non-State Armed Actors in Modern Conflict

Introduction

Traditional ideas of war—where national armies fight under clear legal rules—no longer capture today's reality. Modern conflicts often involve non-state armed actors, including private military companies, transnational insurgent groups, and terrorist organizations. The rise of private and irregular forces has changed how battles are fought, made it harder to know who is responsible for violence, and raised serious concerns about ethics, accountability, and global stability. DISEC delegates are tasked with examining this complex landscape, looking at weak regulations, gaps in oversight, and the diplomatic tools that could help reduce the threats these actors pose.

Historical Analysis

After the Cold War, many soldiers were left without armies to serve in, while new security gaps appeared around the world. This created demand for private military services. Private Military Companies (PMCs) stepped in to perform jobs that had once been done only by states, such as providing logistics, intelligence, training, cybersecurity, and even direct combat support. A well-known example is Executive Outcomes, a South African PMC that operated in Angola and Papua New Guinea. Its involvement disrupted regional stability and showed how dangerous private forces could become when operating with little oversight.

In the early 2000s, oversight and accountability for these actors were still weak. For instance, investigations in Afghanistan found that some U.S.-hired security firms cooperated with local warlords. Instead of creating stability, these partnerships often made conflict zones more volatile and undermined international efforts to restore order. The growing influence of PMCs raised serious legal and diplomatic concerns.

At the same time, non-state armed groups such as militias and insurgencies expanded their reach across borders. These groups often overlap with PMCs and illicit networks, creating a complex web of actors that blur the lines between state and non-state power.

Past International Actions

International law has provided some tools to address the rise of non-state armed actors, but enforcement remains weak. One major step was the 2001 UN Mercenary Convention, which bans the recruitment, use, financing, and training of mercenaries. However, only a small number of states have ratified it, limiting its global impact.

Another effort is the Montreux Document (2008), a non-binding agreement that lays out best practices for states working with PMCs in armed conflict. It highlights the importance of checking a company's credentials, prosecuting violations, and making sure personnel follow international rules.

Building on this, the International Code of Conduct for Private Security Service Providers was created as a voluntary set of standards. It emphasizes respect for human rights, due diligence, and corporate accountability. It also involves oversight from governments and civil society, encouraging companies to meet higher ethical standards even without binding laws. Despite these steps, no measure so far has fully solved the problem. Binding treaties have limited participation, voluntary codes lack enforcement, and universal regulation is still absent. Because PMCs and armed groups often operate across borders, jurisdictional issues and competing geopolitical interests make states hesitant to regulate too strictly. These gaps show why continued international dialogue and innovative solutions are urgently needed to address the evolving role of non-state armed actors in global security

Remaining Challenges

Firstly, PMCs operate in legal gray zones, caught between the categories of civilian, combatant, and unlawful actor. International Humanitarian Law (IHL)—the body of rules that regulates armed conflict and protects civilians during war—offers only limited guidance in such cases, especially regarding who is responsible for PMC actions and how accountability should be enforced.

Secondly, existing international frameworks have limited reach. Many of the states and organizations that hire or use PMCs are not parties to agreements like the UN Mercenary Convention or the Montreux Document. Even in countries that have signed on, enforcement is often inconsistent and weak.

Thirdly, PMCs are sometimes tied to state interests and resource extraction, which can fuel instability in fragile regions. For example, Russia’s Wagner Group has operated in places like the Central African Republic, raising concerns about corporate complicity, exploitation of resources, and geopolitical maneuvering.

Finally, non-state insurgent and terrorist groups continue to challenge state sovereignty and resist conventional systems of control. Their activities increase instability at both the regional and global levels, making international security even harder to maintain.

Next Steps

Delegates are encouraged to explore ways to close the gaps that remain in regulating and overseeing private military contractors (PMCs) and transnational armed groups. This could include strengthening national licensing systems for PMCs and ensuring that humanitarian standards are built into their operations. Another question is how domestic laws might better align with international frameworks such as the Montreux Document and the International Code of Conduct, and whether greater consistency could improve accountability.

Transparency is another priority. Delegates may debate how information about PMC contracts and activities in conflict zones could be made more accessible, as well as what kinds of independent oversight would be most effective.

At the international level, delegates could also consider whether the UN Mercenary Convention should be expanded in scope or supported by wider state participation.

In fragile regions, discussion might include whether rapid-response forces—whether state-based or involving non-state actors—could be deployed under a UN mandate with strict oversight. The broader challenge of transnational armed groups also raises questions about capacity-building, peace negotiations, and regional cooperation.

The goal is to identify approaches that balance stability, sovereignty, humanitarian protection, and accountability, while leaving space for new and innovative solutions in the future.

Questions to Consider

1. How can international norms be adapted to clarify the legal status of PMC personnel and reinforce accountability?
2. What oversight mechanisms would meaningfully regulate PMC activity without undermining security needs?
3. How can states and the UN build greater transparency around PMC contracts, especially in high-conflict areas?
4. What strategies can counter the exploitation of conflict zones by PMCs and their sponsors for resource extraction or political gain?
5. In dealing with transnational armed groups, how can disarmament, demobilization, and reintegration efforts be strengthened to reduce destabilizing private or insurgent capacities?

References (Topic I)

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

"Disarmament in the General Assembly." *United Nations Office for Disarmament Affairs*, disarmament.unoda.org/general-assembly/

Hogeveen, Bart. "The UN Norms of Responsible State Behaviour in Cyberspace." *The UN Norms of Responsible State Behaviour in Cyberspace*, Mar. 2022, documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf.

"2015 UN GGE - Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174)." *Digital Watch Observatory*, 3 Nov. 2023, dig.watch/resource/un-gge-report-2015-a70174

"International Law Applies to Cyber Operations, Tallinn Manual 2.0 Reaffirms." *CCDCOE*, ccdcoe.org/news/2017/international-law-applies-to-cyber-operations-tallinn-manual-2-0-reaffirms/.

Hill, Amanda G. "The Ultimate Challenge: Attribution for Cyber Operations." *The Ultimate Challenge: Attribution for Cyber Operations*, www.airuniversity.af.edu/Portals/10/AUPress/Papers/WF_70_HILL_THE_ULTIMATE_CHALLENGE_ATTRIBUTION_FOR_CYBER_OPERATIONS.PDF

Banks, William. *Cyber Attribution and State Responsibility*, 2021, digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2980&amp;context=ils

"About Cyber Capacity Building." *The GFCE*, 11 Mar. 2025, thegfce.org/about-cyber-capacity-building/

The Convention on Cybercrime (Budapest Convention, ETS No. 185) and Its Protocols, www.coe.int/en/web/cybercrime/the-budapest-convention

Newman, Lily Hay. "Why Is It so Hard to Prove Russia Hacked the DNC?" *Wired*, Conde Nast, 24 Dec. 2016, www.wired.com/2016/12/hacker-lexicon-attribution-problem/

References (Topic II)

Private Military and Security Companies (PMSCS), 2024, www.dcaf.ch/sites/default/files/publications/documents/DCAF_BKG_26_PrivateMilitarySecurityCompanies.pdf.

"The Practical Guide to Humanitarian Law." *Doctors without Borders | The Practical Guide to Humanitarian Law*, guide-humanitarian-law.org/content/article/3/private-military-companies/

"United Nations Mercenary Convention." *Wikipedia*, Wikimedia Foundation, 3 Aug. 2025, en.wikipedia.org/wiki/United_Nations_Mercenary_Convention

"Montreux Document." *Wikipedia*, Wikimedia Foundation, 27 Jan. 2025, en.wikipedia.org/wiki/Montreux_Document

"International Code of Conduct for Private Security Service Providers." *Wikipedia*, Wikimedia Foundation, 17 Mar. 2025, en.wikipedia.org/wiki/International_Code_of_Conduct_for_Private_Security_Service_Providers

Gómez del Prado, José L. "A United Nations Instrument to Regulate and Monitor Private Military and Security Contractors." *Notre Dame Journal of International & Comparative Law*, 2011, scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1012&amp=&context=ndjicl.

Bodurtha, Molly. "An Obligation to Regulate: How Private Military Companies Embolden Conflict with Impunity from the Middle East to Central Africa." *Columbia Journal of Transnational Law*, Columbia Journal of Transnational Law, 1 Apr. 2022, www.jtl.columbia.edu/bulletin-blog/an-obligation-to-regulate-how-private-military-companies-embolden-conflict-with-impunity-from-the-middle-east-to-central-africa.

Feffer, John. "Sudan: Toward a World Ruled by Non-State Actors - FPIF." *Foreign Policy In Focus*, 30 Mar. 2025, fpif.org/sudan-toward-a-world-ruled-by-non-state-actors/

Armed Non-State Actors: Current Trends & Future Challenges, www.files.ethz.ch/isn/144858/ANSA_Final.pdf

Ackerman, Spencer. "Taliban Allies, Warlord Flunkies Guard U.S. Bases." *Wired*, Conde Nast, 7 Oct. 2010, www.wired.com/2010/10/taliban-allies-warlord-flunkies-guard-u-s-bases/