Background Guide

Disarmament and International Security Committee (DISEC)

ACMUN'25

Letter from the Executive Board

Dear Delegates,

We welcome you to The Disarmament and International Security Committee (DISEC)at ACMUN 25'!
As members of the United Nations Human Rights Council, you shall be tasked with discussing and deliberating on the following Agenda:

Addressing State-Sponsored Cyber Warfare and Its Threats to International Security.

This background guide is not to be treated as exhaustive research on the agenda, but instead just as an effort to provide a short yet comprehensive description of the committee and the nuances within the agenda. We encourage and expect each delegate to explore topics/aspects of the agenda not covered within this guide. Regarding the topics mentioned in this guide, we request delegates to treat them as a starting point for their research.

The following sources of information will be deemed *credible* during this conference:

1) Reuters.
2) Reports published by any: body/committee/affiliated body of the United Nations.
3) Statistics and data reported by certain ***credible*** NGOs or statistical organisations.
4) Any other source the Executive Board may deem admissible during committee including information provided by government reports and government-funded/affiliated agency reports/articles.

The Executive Board intends to follow the Rules of Procedures enacted in the UNA-USA format, with variations per the committee's needs.

The Executive Board will not intervene in the flow of debate and the matter being discussed in committee. Our primary responsibility shall always remain moderating and ensuring equitable marking. Therefore, it falls upon the delegates themselves to ensure qualitative debate in the committee.
Please do not hesitate to contact the Executive Board before or during the conference if you have any queries about the agenda or the rules of procedure.

We look forward to an exciting and thoughtful debate for these 2 days!

With warm regards,
Shrisai Hari and Dhruv Bajaj

Introduction to the Committee

The **Disarmament and International Security Committee (DISEC)**, also known as the **First Committee of the United Nations General Assembly**, plays a critical role in promoting international peace and security. It focuses primarily on disarmament, the regulation of global armaments, and addressing threats that jeopardize global stability. DISEC works in tandem with other international bodies such as the United Nations Office for Disarmament Affairs (UNODA), the Conference on Disarmament, and various regional security organizations to formulate policies that reduce the threat of conflict.

Unlike other UN bodies with enforcement powers, DISEC primarily operates through the drafting of non-binding resolutions that reflect the consensus and collective opinion of the international community. These resolutions can pave the way for treaties and global norms, making DISEC a vital platform for diplomacy and agenda-setting on security matters.

As warfare continues to evolve, DISEC has expanded its scope to address emerging challenges, including the militarization of outer space, autonomous weapons systems, and cyber warfare. In particular, **state-sponsored cyber warfare** has emerged as a major security concern, blurring the line between espionage and armed conflict. The increasing reliance on digital infrastructure across military, governmental, and civilian sectors makes it imperative for DISEC to develop comprehensive strategies to address cyber threats.

Introduction to the Agenda

The 21st century has witnessed a profound transformation in the nature of conflict. Today, wars are no longer fought solely on the battlefield with guns and tanks; they are waged silently behind screens, through lines of malicious code and covert digital operations. Among the most pressing threats in this new era of conflict is **state-sponsored cyber warfare**—a form of cyber aggression that is planned, executed, or supported by nation-states to gain strategic advantage over rivals, disrupt international stability, or project power without overt confrontation.

Unlike conventional warfare, cyber warfare exploits the interconnectedness of modern society. States now possess the ability to penetrate critical infrastructure, manipulate elections, steal sensitive data, and paralyze national defense systems—all without crossing physical borders or leaving easily traceable fingerprints. Notable examples include the alleged Russian interference in foreign democratic processes, the Stuxnet virus reportedly developed by the U.S. and Israel to target Iran's nuclear program, and North Korean cyber-attacks aimed at financial institutions and private corporations.

One of the most significant challenges in addressing state-sponsored cyber warfare is **attribution**—identifying the true source of an attack. Unlike traditional armed conflicts, cyber operations can be routed through multiple jurisdictions and masked using sophisticated tools, making it difficult to hold perpetrators accountable. This lack of accountability poses serious questions for international law, particularly around sovereignty, proportionality, and legitimate retaliation.

Currently, there is no universally binding treaty that governs state behavior in cyberspace. Efforts such as the Tallinn Manual, the UN Group of Governmental Experts (UNGGE), and the Open-Ended Working Group (OEWG) have made progress in establishing voluntary norms and principles. However, the absence of enforceable international frameworks continues to leave gaps that malicious state actors can exploit.

The Legalities around the Agenda

Cyber warfare represents an unprecedented challenge to the international legal framework. Traditional laws of war—designed for physical, kinetic conflict—are being tested in a domain where attribution is difficult, sovereignty is blurred, and attacks can be launched at the speed of a keystroke. While some legal structures have attempted to address aspects of cyber activity, there remains no binding, universally accepted international treaty that comprehensively governs **state behavior in cyberspace**. This section outlines the existing legal instruments, their limitations, and the key legal debates surrounding cyber warfare.

I. The United Nations Charter

The UN Charter is the bedrock of international law on the use of force. Two specific provisions are relevant to cyber operations:

- **Article 2(4)** prohibits the use of force against the territorial integrity or political independence of any state. The question arises: can a cyber attack that disables a country's electrical grid or causes economic paralysis be considered a "use of force"?

- **Article 51** allows for self-defense if an armed attack occurs. If a cyber operation causes effects equivalent to a missile strike or widespread destruction, can it justify a kinetic (military) response under the right to self-defense?

The ambiguity in applying these articles to cyberspace is a core challenge. Many experts argue that **intent, scale, and impact** should be the deciding factors, but consensus is lacking.

II. International Humanitarian Law (IHL)

IHL governs the conduct of armed conflict and aims to protect civilians and restrict means of warfare. The **Geneva Conventions**, for example, prohibit attacks on civilian infrastructure like hospitals, water systems, and power grids.

In the cyber realm, a malware attack targeting a hospital's systems during an armed conflict could be considered a violation of IHL. However, many cyber operations occur during peacetime or in the "grey zone" between peace and war, leading to legal uncertainty. Further, cyber tools are dual-use—they can support both civilian and military functions—making them harder to regulate under IHL.

III. Sovereignty and Non-Intervention

Two key customary international law principles also apply:

- **Sovereignty**: States have exclusive control over activities within their territory.
- **Non-intervention**: States should not interfere in the internal affairs of other states.

Cyber intrusions into foreign servers, espionage operations, or election interference may violate these principles. However, most cyber espionage activities have traditionally been treated as unfriendly but not illegal, creating loopholes for state actors.

IV. The Tallinn Manual

The **Tallinn Manual** (Tallinn 1.0 in 2013 and Tallinn 2.0 in 2017) is the most significant non-binding effort to interpret how existing international law applies to cyber warfare. Drafted by a group of legal and military experts, it covers topics such as:

- Attribution and state responsibility
- Thresholds for use of force and armed conflict
- Rules on neutrality and countermeasures
- Due diligence in preventing harm originating from a state's cyber infrastructure

While it is **not an official UN document** and has no legal force, the Tallinn Manual is widely respected and forms a reference for many states and organizations. However, it also reveals deep disagreement among experts, especially on when a cyber operation crosses the threshold of an "armed attack."

V. Budapest Convention on Cybercrime (2001)

The **Budapest Convention** is the first international treaty seeking to address cybercrime through harmonized laws and enhanced cooperation. It focuses on crimes like unauthorized access, data interference, and system intrusion.

However, the Convention's relevance to cyber warfare is limited because:

- It targets **criminal behavior**, not state-led military operations.
- Major cyber powers like **Russia, China, and India** are not signatories, undermining its global effectiveness.

VI. UN Initiatives: GGE and OEWG

The **UN Group of Governmental Experts (UNGGE)** and the **Open-Ended Working Group (OEWG)** are two key platforms discussing norms, rules, and principles for state behavior in cyberspace.

- **UNGGE (2004–2021)**: Developed 11 voluntary norms for responsible state behavior, including not targeting critical infrastructure during peacetime and cooperating to mitigate malicious cyber activity.
- **OEWG (2019–present)**: A more inclusive process involving all UN member states, aimed at building consensus on cybersecurity, capacity-building, and confidence-building measures.

While these forums represent progress, their outcomes remain **non-binding**, and major powers often clash on definitions, thresholds, and enforcement mechanisms.

CASE STUDIES

1. Stuxnet (2010) – US-Israel Operation Targeting Iran's Nuclear Program

Stuxnet remains the most iconic and widely cited example of a state-sponsored cyber weapon deployed in a real-world conflict scenario. Discovered in 2010, the worm was designed specifically to sabotage Iran's uranium enrichment facility at Natanz. Though not officially acknowledged, it is widely believed to have been developed jointly by the United States' NSA and Israel's Unit 8200 under the covert program codenamed "Operation Olympic Games."

The technical sophistication of Stuxnet marked a new era in cyber warfare. The worm exploited four zero-day vulnerabilities in Microsoft Windows—a rarity in itself—and used stolen digital certificates from reputable companies (Realtek and JMicron) to avoid detection. It propagated via USB drives, enabling it to infect air-gapped systems. Once inside the system, Stuxnet specifically targeted Siemens Step7 software used to control programmable logic controllers (PLCs). These PLCs were connected to centrifuges used in uranium enrichment. Stuxnet subtly altered the rotational speed of these centrifuges—making them spin faster or slower than normal—while feeding normal readings to operators, resulting in physical degradation over time.

The worm's payload was surgical in nature: it searched for a very specific hardware configuration, only executing the sabotage if it matched a predefined set of criteria, thus limiting collateral damage. Estimates suggest it destroyed around 1,000 centrifuges at the Natanz facility and delayed Iran's nuclear progress by up to two years.

Stuxnet represented the world's first publicly known instance of malware causing physical destruction. It fundamentally changed the understanding of cyber capabilities—not just as a tool of espionage, but as a strategic military asset capable of inflicting tangible harm without deploying a single soldier. More significantly, it crossed a red line in the cyberspace domain by establishing a precedent: states are now willing to carry out precision cyber strikes against sovereign infrastructure to achieve geopolitical goals.

This case directly relates to the agenda as it introduced cyber sabotage into the realm of international conflict, raising questions around sovereignty, the applicability of International

Humanitarian Law (IHL), and thresholds for the use of force. It remains a textbook example of how cyber weapons can be used to achieve strategic objectives without open warfare and without leaving a clear legal or diplomatic trail. Stuxnet also contributed to the rise of "grey zone" tactics—operations that fall short of outright war but still undermine international security.

2. NotPetya (2017) – Russia's Devastating Supply Chain Attack on Ukraine

In June 2017, a cyberattack initially believed to be ransomware spread rapidly through Ukraine, eventually crippling systems across Europe, North America, and Asia. Dubbed "NotPetya" due to its superficial resemblance to the Petya ransomware family, the malware was later revealed to be a data-wiping wiper masquerading as ransomware. The attack targeted Ukraine's financial, government, and energy sectors and was attributed to the Russian military intelligence unit GRU, specifically APT28 (Fancy Bear).

NotPetya's initial infection vector was a compromised update mechanism of a widely-used Ukrainian accounting software called MeDoc. Once deployed, the malware used multiple lateral movement techniques, including the EternalBlue exploit (developed by the NSA and leaked by the Shadow Brokers), EternalRomance, and credential theft via Mimikatz. It then rewrote the Master Boot Record (MBR) of infected systems, rendering them inoperable.

The malware spread uncontrollably, affecting major global companies such as Maersk (shipping), Merck (pharmaceuticals), FedEx subsidiary TNT Express, and Rosneft (Russian oil). Damages were estimated at over $10 billion globally. Maersk alone reportedly spent over $300 million to recover, needing to reinstall 45,000 PCs, 4,000 servers, and 2,500 applications.

Technically, NotPetya demonstrated how weaponized malware could exploit trusted software supply chains to gain widespread access to networks. Unlike typical ransomware, it lacked any functional decryption mechanism, confirming its purpose was destruction rather than financial gain. It represented an evolution in hybrid warfare, with a clear objective to destabilize Ukraine's economy during ongoing geopolitical tensions, while also showcasing Russia's capability to inflict collateral damage at a global scale.

From an international security standpoint, NotPetya blurs the line between targeted and indiscriminate attacks. Although Ukraine was the principal target, the worm's uncontrolled propagation violated norms of responsible state behavior in cyberspace and endangered critical infrastructure globally. The use of a civilian software company's infrastructure for military objectives sets a dangerous precedent. It also sparked urgent discourse within the UN and among NATO allies about cyber deterrence and collective defense in the digital domain.

3. SolarWinds (2020) – Russian Espionage Through Supply Chain Subversion

The SolarWinds cyber espionage campaign, uncovered in December 2020, is one of the most far-reaching and technically sophisticated supply chain attacks in history. The Russian state-sponsored hacking group APT29, or Cozy Bear, believed to be affiliated with the SVR (Russia's Foreign Intelligence Service), managed to inject malware into the Orion software platform—a network management tool used by over 18,000 entities worldwide.

APT29 compromised SolarWinds' development environment and inserted a backdoor (known as SUNBURST) into Orion software updates. When unsuspecting customers installed the updates, they unknowingly provided access to their internal networks. Once inside, the attackers conducted stealthy reconnaissance, lateral movement, and data exfiltration operations.

Targets included major U.S. federal agencies such as the Departments of State, Treasury, Homeland Security, and Energy, as well as private firms like Microsoft, FireEye, and numerous critical infrastructure providers. The attack went undetected for almost nine months, showcasing the group's deep operational security and mastery of espionage tradecraft. The malware was designed to lie dormant for up to two weeks post-installation and employed domain generation algorithms, IP masquerading, and sophisticated command-and-control infrastructure.

What made SolarWinds particularly alarming was the violation of software supply chain trust. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive, declaring the event a "grave risk" to national security. The scale of compromise demonstrated that even the most secure networks could be penetrated through third-party software dependencies.

This incident spotlights the vulnerability of global digital infrastructure to state-sponsored espionage. While SolarWinds was a cyber espionage operation rather than sabotage, it exposed the lack of global norms regulating cyber behavior, especially regarding acceptable conduct in peacetime. The scale and stealth of the attack intensified calls for new international frameworks to protect critical systems and ensure software integrity, directly aligning with the agenda of addressing state-sponsored threats to global security.

4. Russo-Ukrainian Hybrid Cyber Campaigns (2014–Present)

Since the annexation of Crimea in 2014, Ukraine has been a laboratory for Russian cyber-warfare operations, integrating digital attacks into broader hybrid warfare strategy. The Russian Federation's state-backed actors, notably Sandworm (APT28/29), have executed sustained campaigns targeting Ukrainian power grids, election infrastructure, media outlets, and military systems.

One of the most alarming incidents occurred in December 2015, when Ukraine experienced the first known blackout caused by a cyberattack. Using BlackEnergy malware, attackers gained access to three regional power distribution centers, remotely opened circuit breakers, and cut power to 230,000 people. In 2016, a second blackout occurred using a more advanced malware strain known as Industroyer or CrashOverride. This malware directly interacted with ICS/SCADA protocols like IEC 101 and IEC 104—specifically designed for power grids.

These attacks were accompanied by phishing campaigns, data leaks, and defacements, forming a coherent strategy to disrupt the country's political and civilian functions. The culmination of these efforts was seen again during the full-scale invasion of Ukraine in 2022, where Viasat satellite modems were disabled on the eve of the kinetic assault, hindering Ukrainian communications.

The Russo-Ukrainian cyberwarfare theater is a living example of how state-sponsored cyber operations have evolved from isolated incidents into strategic tools of warfare. These cyberattacks have targeted critical infrastructure, sown confusion during wartime, and tested the effectiveness of international coordination and resilience strategies. Despite the clear aggressor, international attribution and accountability remain elusive, underscoring the gaps in enforcement mechanisms under current international law.

These campaigns vividly demonstrate how cyber warfare is not limited to espionage or disruption but is now an integral pillar of military strategy. For international security, this raises urgent questions about proportionality, sovereignty, and the need for treaty-level deterrents against cyberattacks targeting civilians and infrastructure.

Conclusion

State-sponsored cyber-warfare poses a transformative and escalating threat to international security. The technical sophistication—exploiting zero-days, supply chains, command-and-control networks—allows for disruption, espionage, sabotage, and military augmentation without kinetic deployment. Past case studies show:

- **Physical consequences** (Stuxnet, grid outages in Ukraine),
- **Strategic impact** (shaping public opinion, elections, high-profile events),
- **Economic ripple effects** (NotPetya, WannaCry).

The **grey-zone alignment**—below armed conflict yet above mere crime—presents an enforcement challenge. States increasingly rely on cyber tactics to achieve geopolitical goals, often retreating into anonymity. Yet with evolving attribution tools, improved techno-legal cooperation, and developing international confidence-building measures, this space can be regulated.

The international community stands at a crossroads: either perpetuate an ungoverned cyber arms race, or formalize norms, attribution standards, response mechanisms, and collective defense protocols—through the UN, OEWG transformation, or new treaties.

A stronger global framework would:

- Clarify **when cyberattacks trigger legal thresholds** (armed attack, breach of sovereignty, humanitarian violation).
- Define **state accountability** for both direct and proxy cyber operations.
- Mandate **assistance, transparency, and capacity-building**, particularly for vulnerable nations.
- Establish **cooperative backstops** (cyber peacekeeping, "blue helmets", incident-response coordination).
- Provide **enforcement and remediation paths**, including clear governance through the Security Council.

Ultimately, cyber-warfare isn't just a technical domain—it's a critical battlefield of geopolitics, economic levers, and civilian risk. The international system must evolve legally, operationally, and normatively to meet that reality

QARMA

When does a cyber act qualify as an armed attack under Article 2(4) of the UN Charter?

How to interpret current norms like the eleven GGE principles, the Tallinn Manual, or the OEWG's permanent mechanism?

What duties exist for states to prevent proxies and vigilantes from operating from within their borders?

How to enforce the prohibition against states allowing their territory to be used as a launch pad for harmful cyber operations?

How to apply IHL in cyber warfare—principles of distinction, proportionality, necessity?

What are the governance structures for a UN Cybersecurity Treaty, cyber-peacekeeping mechanisms, or a digital blue helmets corps?

Recommended Sources for Preliminary Research

Here are **primary resources** from UN bodies, Reuters, and Al Jazeera to anchor your research:

- **UN Security Council meeting documents** (e.g., Resolutions, concept notes, meeting records):
    - Security Council concept note on cyber security and ransomware
    - UN Press release on Resolution 2341 (2017) about threats to critical infrastructure
- **UN OEWG / GGE proceedings**:
    - OECD discussions on IHL and cyber ops
    - OEWG analysis on permanent mechanism and cyber diplomacy
- **AsPI / Tallinn / academic analyses**:
    - UN norms of responsible state behavior
    - Tallinn Manual and international legal frameworks
- **Reuters / Al Jazeera** news investigations:
    - Reuters overview of Israel's Unit 8200
    - Al Jazeera tech coverage of the Stuxnet phenomenon
- **Security Council and think-tank webinars/reports**:
    - Stimson Center on capacity building and humanitarian impacts
    - Cyber peacekeeping research: ArXiv papers on UN "Digital Blue Helmets" and CPK