

ASHOKA MODEL UNITED NATIONS 2026

DISARMAMENT AND INTERNATIONAL SECURITY COMMITTEE (DISEC)

AGENDA Deliberating the Growing Threat of Gray Zone Warfare and the Proliferation of Non-State Armed Actors to International Peace and Security

TABLE OF CONTENTS

1. Introduction to the Committee
2. The Growing Threat of Gray Zone Warfare and the Proliferation of Non-State Armed Actors
 - Statement of the Problem
 - History of the Problem
 - Current Situation
 - What is Gray Zone Warfare?
 - The Strategic Space Between Peace and War
 - State Sponsorship and Proxy Actors
 - Non-State Armed Actors and the Security Environment
 - Illicit Arms Flows and Diversion
 - Terrorist Organisations and Armed Groups
 - Technology and the Changing Character of Conflict
 - Cyber, Information and Political Coercion
 - Sovereignty, Attribution and Accountability
 - Regional Spillovers and Conflict Escalation
 - Humanitarian and Civilian Consequences
 - The Enforcement Gap
3. Case Studies: Gray Zone Warfare and Non-State Armed Actors in Practice
4. Relevant UN Actions
5. Bloc Positions
6. Glossary of Key Terms
7. Questions a Resolution Must Answer
8. Sample Operative Clause Bank
9. Country Research Checklist
10. Suggestions for Further Reading
11. Bibliography

1. INTRODUCTION TO THE COMMITTEE

The First Committee of the United Nations General Assembly, formally known as the Disarmament and International Security Committee (DISEC), deals with disarmament, global security challenges and threats to international peace. Its mandate includes questions concerning disarmament, the regulation of armaments, international security and cooperative arrangements designed to strengthen stability.

DISEC works alongside other parts of the UN disarmament machinery, particularly the United Nations Office for Disarmament Affairs (UNODA), the Conference on Disarmament, and the UN Disarmament Commission.

For this agenda, however, delegates must understand an important institutional distinction:

DISEC discusses, recommends and develops international norms and cooperative mechanisms; it is not the UN Security Council.

The Security Council possesses enforcement powers under the UN Charter, including sanctions and arms embargoes under Chapter VII. DISEC resolutions are therefore primarily recommendatory rather than coercive.

WHAT THIS COMMITTEE IS REALLY DEBATING

The issue is not simply "how do we stop terrorism?" Nor is it simply "how do we regulate weapons?"

The central question is:

How can the international community respond to security threats that deliberately operate below the threshold of conventional armed conflict, particularly when states use or support non-state actors while maintaining plausible deniability?

Delegates must balance:

- state sovereignty and territorial integrity;
- the right of states to defend themselves;
- the prohibition on the use of force;
- counter-terrorism obligations;
- prevention of illicit arms transfers;
- accountability for state sponsorship;
- civilian protection;
- attribution of hostile activity;
- technological developments;

- and the limits of existing international institutions.

The strongest solutions will therefore not merely call for "greater cooperation." They will identify who should act, under which framework, using what mechanism, with what verification and accountability.

A NOTE ON COMMITTEE PROCEDURE FOR THIS AGENDA

Because this topic sits at the intersection of several existing legal regimes (arms control, counter-terrorism, use-of-force law, and cyber norms), delegates frequently make one of two mistakes:

1. **Over-legalizing the debate** — treating DISEC as though it can issue binding legal determinations of state responsibility (it cannot; that is closer to the function of the ICJ or the Security Council).
2. **Under-legalizing the debate** — ignoring existing frameworks entirely and proposing vague new bodies that duplicate UNODA, the CTC, or the 1540 Committee.

The strongest delegates will thread this needle: they will use precise language, cite the correct existing mechanism for each sub-problem, and propose realistic recommendatory action that a General Assembly committee can actually pass.

2. THE GROWING THREAT OF GRAY ZONE WARFARE AND THE PROLIFERATION OF NON-STATE ARMED ACTORS

STATEMENT OF THE PROBLEM

International conflict is increasingly characterised by activities that do not fit neatly into the traditional categories of peace and war.

States can pursue strategic objectives through combinations of political pressure, economic coercion, cyber operations, information manipulation, covert activity, proxy forces and other forms of pressure while deliberately avoiding actions that would clearly trigger a conventional military response.

This space is frequently described as the "gray zone" or "gray zone warfare."

The terminology is important but should not be treated as a settled category of international law. Unlike concepts such as aggression, armed attack or international armed conflict, "gray zone warfare" is primarily a strategic and analytical concept rather than a universally codified legal classification.

The problem becomes more complex when states operate through non-state armed actors.

These actors may include armed groups, militias, insurgent organisations, terrorist organisations or other organised groups capable of exercising violence independently of a conventional state military structure.

Their existence creates several interconnected challenges:

- attribution of responsibility;
- illicit weapons transfers;
- proxy warfare;
- territorial sovereignty;
- terrorism financing;
- border security;
- proliferation and diversion;
- accountability for sponsors;
- and escalation between states.

The UN has repeatedly recognised the destabilising effects of illicit arms flows. The Organisation notes that illicit transfers can destabilise regions, facilitate violations of arms embargoes and contribute to violence and human rights abuses.

The challenge for DISEC is therefore to determine how existing international frameworks can be strengthened and connected without creating an undefined or overly broad international mandate.

THREE TERMS TO KEEP SEPARATE

TERM	WHAT IT MEANS	WHY IT MATTERS
Gray Zone Warfare	Strategic activity intended to advance political or security objectives while remaining below, around or deliberately ambiguous in relation to the threshold of conventional armed conflict.	Creates problems of attribution, deterrence and legal classification.
Hybrid Warfare	A broader concept involving the coordinated use of military and non-military instruments to pursue strategic objectives.	May overlap with gray-zone activity but is not identical to it.
Non-State Armed Actor	An organised armed entity that is not formally part of the armed forces of a state.	Creates questions regarding control, responsibility, recognition and accountability.

DELEGATE SHORTCUT

- Do not treat every non-state actor as a terrorist organisation.
 - Do not treat every proxy as legally equivalent to a state military.
 - Do not treat every gray-zone activity as an act of war.
 - And do not assume that the use of a non-state actor automatically removes state responsibility.
-

HISTORY OF THE PROBLEM

From Conventional War to Indirect Conflict

Traditional international security frameworks were largely constructed around states as the principal actors in international conflict.

The UN Charter established a system centred on sovereign equality, peaceful settlement of disputes and restrictions on the use of force.

Yet armed conflicts throughout the twentieth century demonstrated that states could influence conflicts without directly deploying conventional forces.

The Cold War particularly demonstrated the strategic importance of:

- proxy forces;
- covert assistance;
- political influence;
- intelligence operations;
- ideological competition;
- and indirect military involvement.

Rather than confronting one another directly, major powers could support opposing actors in conflicts elsewhere.

This did not eliminate interstate competition. It changed the methods through which that competition occurred.

The Rise of Non-State Armed Actors

The end of the Cold War did not eliminate armed groups.

Instead, civil wars, state fragility, terrorism, organised crime and regional conflicts produced environments in which non-state armed actors could acquire significant political and military influence.

The international community increasingly confronted situations in which:

- governments lacked effective control over territory;
- armed groups operated across borders;
- weapons moved through illicit networks;
- terrorist organisations developed transnational structures;
- and external states supported local actors.

The illicit proliferation of small arms and light weapons became an especially important concern because these weapons are relatively portable and can sustain armed violence long after a conflict begins.

The UN Programme of Action on Small Arms and Light Weapons was adopted in 2001 to prevent, combat and eradicate the illicit trade in small arms and light weapons in all its aspects.

The International Tracing Instrument subsequently strengthened international cooperation concerning the identification and tracing of illicit small arms and light weapons.

The Post-9/11 Security Environment

The terrorist attacks of 2001 fundamentally changed the international counter-terrorism framework.

Security Council Resolution 1373 established a broad international counter-terrorism framework and created the Counter-Terrorism Committee to monitor implementation by Member States.

The international community subsequently expanded its focus toward:

- terrorist financing;
- border controls;
- terrorist travel;
- illicit trafficking;
- terrorist recruitment;
- and international cooperation.

This also strengthened the relationship between disarmament, arms control and counter-terrorism.

The 2010s–2020s: The "Gray Zone" Enters Mainstream Strategic Vocabulary

Although indirect and ambiguous forms of conflict are not new, the specific term "gray zone" became widespread in strategic and defence literature roughly from the mid-2010s onward. This period was marked by:

- the annexation of Crimea and the subsequent conflict in eastern Ukraine, where unmarked forces and local proxies complicated attribution;

- island-building and militarisation activity in the South China Sea conducted through a combination of military, paramilitary (coast guard and "maritime militia") and civilian assets;
- an increase in state-linked cyber intrusions against critical infrastructure, elections and financial systems;
- the expansion of private military and security companies operating in conflict and post-conflict states;
- growing use of economic coercion (trade restrictions, investment screening, resource leverage) as a tool of strategic pressure short of armed force.

This period is important for delegates because it shows that gray-zone competition is not confined to any single region or bloc — it has been used, alleged, or debated in relation to conduct by multiple major and middle powers, which is precisely why DISEC struggles to agree on a single definition.

CURRENT SITUATION

1. WHAT IS GRAY ZONE WARFARE?

Gray-zone activity refers to strategic behaviour designed to achieve objectives without entering an unambiguous conventional war.

The concept is deliberately broad. Examples may include:

- political coercion;
- economic pressure;
- cyber activity;
- disinformation;
- covert influence;
- proxy activity;
- interference with political processes;
- and other forms of coercive statecraft.

NATO's 2024 reference curriculum similarly treats "grey zone," "hybrid warfare," information warfare and related concepts as overlapping but contested terminology rather than a single universally defined phenomenon.

THE CORE PROBLEM

The ambiguity can itself become strategically useful.

If responsibility cannot be established clearly:

Attribution becomes difficult → response becomes uncertain → deterrence weakens → escalation risks increase.

2. THE STRATEGIC SPACE BETWEEN PEACE AND WAR

Traditional security policy often assumes:

Peace → Crisis → War

Gray-zone competition complicates this model.

A state may attempt to remain in an intermediate space where its actions are:

- hostile but difficult to attribute;
- coercive but not conventionally military;
- damaging but legally contested;
- or conducted through intermediaries.

This creates a major diplomatic dilemma. A response that is too weak may encourage further coercion. A response that is too strong may accelerate escalation.

THE QUESTION FOR DISEC

How can states establish credible thresholds and response mechanisms without declaring every hostile act an act of war?

3. STATE SPONSORSHIP AND PROXY ACTORS

One of the most difficult aspects of gray-zone conflict is the relationship between states and non-state armed actors.

A state may:

- provide political support;
- provide financial assistance;
- provide training or logistical support;
- facilitate access to territory;
- provide equipment;
- or otherwise enable an armed actor.

However, the existence of assistance does not automatically answer the legal question of state responsibility.

Delegates must therefore distinguish between:

CONCEPT

DEFINITION

SUPPORT	A state provides assistance to an actor.
CONTROL	A state exercises a legally significant degree of control over an actor or operation.
ATTRIBUTION	An act can legally be attributed to the state under the applicable rules of international responsibility.
PROXY WARFARE	A state uses or supports another actor to pursue strategic objectives while maintaining a degree of separation.

These concepts overlap, but they are not interchangeable.

Delegate note: International legal scholarship has long debated the appropriate threshold for attributing a non-state actor's conduct to a sponsoring state — ranging from stricter "effective control" standards to broader "overall control" standards. DISEC does not need to resolve this legal debate, but strong delegates should be aware that it exists and that their resolution should not implicitly assume one standard is settled law.

4. NON-STATE ARMED ACTORS AND THE SECURITY ENVIRONMENT

Non-state armed actors can become major security challenges when they possess:

- territorial influence;
- independent financing;
- access to illicit networks;
- cross-border operational capacity;
- political legitimacy among sections of a population;
- or relationships with external state sponsors.

Their proliferation can weaken state institutions and make conventional diplomacy more difficult.

The problem is particularly severe when armed groups operate across borders.

A state may therefore face an armed threat originating outside its territory while the neighbouring state may claim that it lacks effective control over the actor.

This produces a difficult question:

When does an armed group's activity become an international security issue requiring collective action?

5. ILLICIT ARMS FLOWS AND DIVERSION

The proliferation of non-state armed actors is closely connected to the diversion of conventional arms.

Diversion occurs when legally produced or transferred arms ultimately reach unauthorised recipients or illicit markets.

This may occur through:

- inadequate stockpile management;
- weak transfer controls;
- fraudulent documentation;
- corruption;
- conflict-related capture;
- or trafficking networks.

The UN's Programme of Action and International Tracing Instrument focus heavily on strengthening national controls, international cooperation, marking, record-keeping and tracing.

WHY THIS MATTERS

A weapons-control system can fail even if the original transfer was formally legal. Therefore:

Legal transfer ≠ guaranteed lawful end-user.

The international community must consider the entire transfer chain.

6. TERRORIST ORGANISATIONS AND ARMED GROUPS

Terrorist organisations represent one particularly important category of non-state armed actor.

However:

Non-state armed actor ≠ terrorist organisation.

The international community does not have one single universal legal category covering every armed non-state group.

Terrorist organisations are subject to a distinct international counter-terrorism framework, including obligations arising from Security Council resolutions.

Resolution 1373 established obligations relating to preventing and suppressing terrorist financing and strengthening international cooperation against terrorism.

DISEC should therefore avoid creating a framework so broad that legitimate questions concerning armed conflict, insurgency, terrorism and organised crime become indistinguishable.

7. TECHNOLOGY AND THE CHANGING CHARACTER OF CONFLICT

Technology has expanded the number of ways in which states and non-state actors can exert influence.

Modern security concerns increasingly include:

- cyber operations;
- autonomous and semi-autonomous technologies;
- commercially available technologies (including small drones);
- information manipulation;
- digital surveillance;
- artificial intelligence;
- and remotely operated systems.

The UN disarmament agenda increasingly addresses emerging technologies alongside conventional arms control and international security.

For DISEC, the challenge is not simply technological development. It is governance.

Questions include:

- Who is responsible when technology is used by an unidentified actor?
- How can states distinguish legitimate civilian technologies from security threats?
- How should international norms address emerging capabilities without restricting peaceful technological development?
- How can accountability be preserved when technology enables anonymity?

Additional consideration: The commercial availability of small unmanned aerial systems (drones) has been a particularly fast-moving concern. Non-state armed groups in several conflict-affected regions have been documented using modified commercial drones for surveillance and attack purposes, raising a governance question that predates most existing arms-control instruments, which were designed with conventional weapons systems in mind.

8. CYBER, INFORMATION AND POLITICAL COERCION

Gray-zone competition frequently involves actions that target the political or informational environment rather than physical territory.

These may include:

- manipulation of information;
- attempts to undermine public trust;
- interference with institutions;
- cyber-enabled disruption;
- or coordinated influence operations.

The strategic objective may be to weaken an opponent without creating the immediate conditions for conventional military escalation.

This creates a particularly difficult attribution problem.

A cyber incident may be:

- technically identifiable;
- operationally traceable;
- politically attributable;
- or legally attributable.

These are four different questions.

Delegate note: The UN Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications have both worked to build normative frameworks for responsible state behaviour in cyberspace. Delegates working on the cyber dimension of this agenda should be aware of these parallel processes rather than proposing to duplicate them.

9. SOVEREIGNTY, ATTRIBUTION AND ACCOUNTABILITY

The international system is built around sovereign states.

Gray-zone conflict complicates sovereignty because harmful activities can originate outside a state's territory while remaining difficult to attribute.

Delegates should therefore distinguish:

CONCEPT	QUESTION IT ANSWERS
Attribution	Who carried out the action?
Responsibility	Who can legally be held responsible?
Accountability	What mechanism exists to respond?
Enforcement	Who has the authority to impose consequences?

A strong DISEC resolution should not collapse all four into a single concept.

10. REGIONAL SPILLOVERS AND CONFLICT ESCALATION

Non-state armed actors can transform local disputes into regional security crises.

An armed group may:

- operate across borders;
- obtain support from external actors;
- move personnel or resources between jurisdictions;
- destabilise neighbouring states;

- or trigger retaliatory action.

The result can be a cycle:

Local conflict → external support → armed-group expansion → cross-border insecurity → interstate tensions → regional escalation.

The international community must therefore address the conditions that allow armed actors to expand, rather than only responding after escalation occurs.

11. HUMANITARIAN AND CIVILIAN CONSEQUENCES

Gray-zone competition is often discussed in strategic terms.

However, civilians ultimately experience its consequences.

Protracted conflict involving armed groups can result in:

- displacement;
- destruction of infrastructure;
- disruption of essential services;
- economic instability;
- restrictions on humanitarian access;
- and prolonged insecurity.

The availability of weapons can also sustain conflicts after political settlements become possible.

This makes arms management, conflict prevention, disarmament and reintegration relevant to long-term peacebuilding.

Delegates should also be mindful that counter-terrorism and arms-interdiction measures, if drafted too broadly, can inadvertently restrict legitimate humanitarian operations (for example, by making it harder for humanitarian organisations to engage with authorities that control territory where aid is needed). A strong resolution should include language protecting principled humanitarian action alongside its security provisions.

12. THE ENFORCEMENT GAP

The international community already possesses multiple instruments.

The problem is often implementation and coordination.

There are frameworks addressing:

- illicit arms trafficking;
- terrorism;

- WMD proliferation;
- arms transfers;
- sanctions;
- peacekeeping;
- conflict prevention;
- and disarmament.

Yet these frameworks operate through different institutions.

The challenge for DISEC is therefore:

How can existing mechanisms be connected without duplicating mandates or creating an unrealistic new international bureaucracy?

3. CASE STUDIES: GRAY ZONE WARFARE AND NON-STATE ARMED ACTORS IN PRACTICE

Delegates should use these case studies as illustrative background for understanding the mechanics of gray-zone activity — not as a basis for naming or condemning specific states in the resolution text itself, which would exceed the scope of a General Assembly recommendatory resolution and risk making the document unpassable in committee.

Proxy and Militia Networks in the Middle East

Several state and non-state actors in the Middle East have developed long-standing relationships between governments and armed groups operating across national boundaries, involving financial support, weapons supply, and training. These relationships illustrate the difficulty of applying "support," "control" and "attribution" as distinct legal categories: external backers have sometimes exercised significant influence over strategic decisions while the armed groups retain their own independent chains of command, local legitimacy and, in some cases, formal or informal political representation within their home states.

Private Military and Security Companies in Africa

The growth of private military and security companies operating in fragile and conflict-affected African states has raised distinct governance questions. These entities may formally be private commercial actors while maintaining close relationships with sponsoring governments, complicating both attribution of their conduct and application of existing arms-transfer and end-use monitoring frameworks, which were largely designed around state-to-state transfers.

Maritime Gray-Zone Activity

In several contested maritime areas, states have used a combination of naval forces, coast guard vessels and ostensibly civilian fishing fleets to assert territorial claims and pressure other states, without engaging in conventional naval combat. This "maritime militia" model illustrates how gray-zone tactics can extend disarmament and security debates beyond land-based arms flows into questions of civilian-military dual use and freedom of navigation.

Cyber Intrusions Against Critical Infrastructure

Several high-profile cyber incidents over the past decade — targeting energy grids, financial systems, healthcare institutions and election infrastructure — have demonstrated how technically sophisticated, state-linked actors can achieve strategic disruption while maintaining varying degrees of deniability. These incidents are frequently attributed by private cybersecurity firms and some governments with differing degrees of confidence, illustrating the gap between technical, political and legal attribution discussed above.

Non-State Armed Actors in the Sahel

The Sahel region has experienced a significant expansion of non-state armed groups — including violent extremist organisations and community-based militias — operating across porous borders shared by multiple states. Weak state capacity, illicit arms flows (including weapons diverted from other regional conflicts), and cross-border movement of fighters have combined to produce a regional security crisis that individual states have struggled to address unilaterally, illustrating the "local conflict → regional escalation" cycle described above.

Small Arms Diversion in Conflict Zones

Investigations by UN Panels of Experts monitoring various Security Council sanctions regimes have repeatedly documented cases in which weapons originally transferred through lawful channels were subsequently diverted — through capture, resale, or corrupt intermediaries — to sanctioned armed groups or embargoed destinations. These documented cases form much of the evidentiary basis for the Programme of Action's emphasis on stockpile security, marking, and end-use verification.

4. RELEVANT UN ACTIONS

1. FIRST COMMITTEE AND UNODA

The First Committee is the central General Assembly forum for disarmament and international security questions. Its mandate includes principles governing disarmament and regulation of armaments and measures intended to strengthen international stability.

UNODA supports Member States and UN disarmament bodies across nuclear, conventional and emerging security issues. Its work includes conventional arms control, illicit small-arms flows and emerging technologies.

Delegate takeaway: DISEC is most effective when its proposals focus on norms, cooperation, reporting, capacity-building and coordination rather than pretending it can directly enforce Security Council sanctions.

2. PROGRAMME OF ACTION ON SMALL ARMS AND LIGHT WEAPONS

The UN Programme of Action (PoA) provides a framework for preventing, combating and eradicating the illicit trade in small arms and light weapons.

The framework addresses national, regional and international measures.

The 2026 Ninth Biennial Meeting of States specifically examined implementation of the Programme of Action and the International Tracing Instrument, including prevention of diversion to unauthorised recipients and illicit markets.

Why it matters to this agenda

Non-state armed actors frequently benefit from illicit arms flows.

Therefore, stronger:

- record-keeping;
- transfer controls;
- tracing;
- stockpile management;
- border cooperation;
- and international assistance

can reduce opportunities for armed-group proliferation.

3. INTERNATIONAL TRACING INSTRUMENT

The International Tracing Instrument provides a framework for States to identify and trace illicit small arms and light weapons.

The broader principle is simple:

The international community cannot effectively address illicit diversion if it cannot establish where an illicitly recovered weapon originated and how it moved.

For delegates, this makes traceability a useful resolution mechanism.

4. ARMS TRADE TREATY

The Arms Trade Treaty (ATT) regulates the international trade in conventional arms and establishes international standards intended to prevent illicit trade and diversion.

The ATT is relevant because gray-zone conflict and armed-group proliferation can be facilitated by irresponsible or poorly controlled international transfers.

However, delegates should not present the ATT as a universal enforcement mechanism.

A strong proposal should instead ask:

- How can implementation be improved?
- How can reporting be strengthened?
- How can diversion risks be assessed?
- How can states receive technical assistance?
- How can existing frameworks complement one another?

5. SECURITY COUNCIL SANCTIONS AND ARMS EMBARGOES

The Security Council can impose sanctions under Chapter VII, including targeted measures and arms embargoes.

Arms embargoes have been used in situations involving armed groups and conflict zones.

The Security Council has also developed sanctions regimes targeting particular individuals and entities associated with terrorism and armed conflict.

DISEC LIMITATION

DISEC itself cannot impose a Security Council-style mandatory arms embargo.

Delegates should therefore frame DISEC proposals around:

- recommendations;
- implementation support;
- information-sharing;
- capacity-building;
- reporting;
- coordination;
- and strengthening existing international instruments.

6. RESOLUTION 1373 AND COUNTER-TERRORISM

Security Council Resolution 1373 established the Counter-Terrorism Committee and created a broad framework for Member States to strengthen their ability to counter terrorism.

Its relevance to this agenda lies particularly in:

- terrorist financing;
- international cooperation;
- border security;
- and preventing support for terrorist activity.

Delegates should recognise that counter-terrorism is broader than weapons control.

7. RESOLUTION 1540 AND NON-STATE ACTORS

Security Council Resolution 1540 is particularly important when the agenda concerns the possibility of non-state actors acquiring nuclear, chemical or biological weapons and their means of delivery.

Resolution 1540 requires states to refrain from supporting non-state actors seeking to develop, acquire, manufacture, possess, transport, transfer or use such weapons and establishes binding obligations concerning domestic controls and prevention of proliferation.

This provides an important model for discussing:

How can states prevent non-state actors from exploiting gaps in national export, border and material-control systems?

8. UN PEACEKEEPING, DDR AND ARMS MANAGEMENT

Disarmament is not limited to treaties.

In conflict-affected environments, the UN can support:

- disarmament;
- demobilisation;
- reintegration;
- weapons management;
- peacebuilding;
- and institutional recovery.

These approaches are particularly relevant after armed groups enter political settlements.

The objective is not simply to remove weapons. It is to reduce the political and economic incentives that sustain armed mobilisation.

9. EMERGING TECHNOLOGIES AND INTERNATIONAL SECURITY

UN disarmament work increasingly considers emerging technologies and their implications for international security, including autonomous weapon systems and developments in science and technology.

For this agenda, delegates should focus on responsible governance, accountability and international norms, rather than technical specifications of weapons.

10. UN GROUP OF GOVERNMENTAL EXPERTS / OPEN-ENDED WORKING GROUP ON CYBER

The UN has developed parallel processes — the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) — dedicated to building norms of responsible state behaviour in the use of information and communications technologies. These processes have produced consensus reports affirming that international law, including the UN Charter, applies in cyberspace, and have proposed a set of voluntary, non-binding norms.

Delegate takeaway: A DISEC resolution addressing the cyber dimension of gray-zone warfare should reference and reinforce these existing processes rather than create a competing or duplicative body.

11. REGIONAL ORGANISATIONS

Regional and sub-regional organisations often play a frontline role in addressing non-state armed actors and illicit arms flows, including through regional arms-control instruments, joint border-security initiatives, and regional early-warning mechanisms. DISEC resolutions can usefully call for closer cooperation between the UN system and relevant regional organisations, recognising that regional bodies frequently have more granular operational knowledge of local armed-group dynamics than global institutions.

DISEC RULEBOOK AT A GLANCE

IF THE ISSUE INVOLVES...	START WITH...	ASK...
Illicit arms flows	UN PoA on SALW	Where are diversion and tracing gaps?
Arms transfers	Arms Trade Treaty	How can responsible transfer standards be implemented?
Weapons diversion	International Tracing Instrument	Can the origin and movement of illicit arms be established?

Terrorist groups	UNSC Resolution 1373	Are financing, border and cooperation mechanisms effective?
WMD proliferation to non-state actors	UNSC Resolution 1540	Are domestic controls preventing proliferation?
Arms embargoes	Security Council sanctions framework	Who has enforcement authority?
Post-conflict armed groups	DDR / peacebuilding mechanisms	How can combatants transition into civilian life?
Gray-zone coercion	UN Charter + international security framework	What threshold and attribution problems arise?
Cyber-enabled coercion	UN GGE / OEWG cyber norms processes	What existing norm applies, and how can implementation be verified?
Emerging technology	UNODA / First Committee	What international norms or safeguards are required?

5. BLOC POSITIONS

The bloc positions below are general analytical starting points. A country may fit more than one category. Delegates must research the assigned state's security environment, alliances, conflict exposure, arms-control commitments and domestic priorities before finalising their position.

1. MAJOR MILITARY POWERS

Likely to emphasise:

- national security;
- strategic deterrence;
- freedom to respond to emerging threats;
- counter-terrorism;
- intelligence cooperation;
- and protection against hostile state activity.

They may support stronger attribution mechanisms while remaining cautious about international rules that could restrict national security operations.

Potential tension: transparency versus operational secrecy.

2. MAJOR EMERGING POWERS

Likely to emphasise:

- sovereignty;
- non-interference;
- territorial integrity;
- opposition to unilateral intervention;
- and equal application of international law.

They may support multilateral mechanisms but resist frameworks that could be interpreted as giving powerful states greater freedom to intervene.

Potential tension: collective security versus sovereignty.

3. STATES DIRECTLY AFFECTED BY NON-STATE ARMED ACTORS

Likely to prioritise:

- border security;
- counter-terrorism;
- intelligence-sharing;
- arms tracing;
- capacity-building;
- and preventing external support to armed groups.

These states may favour stronger international cooperation and more effective mechanisms for preventing armed groups from obtaining resources.

Potential tension: domestic security versus civilian and humanitarian concerns.

4. STATES WITH SIGNIFICANT ARMS-PRODUCTION CAPACITY

Likely to emphasise:

- responsible international transfers;
- export-control systems;
- national sovereignty over defence policy;
- technological development;
- and prevention of diversion.

They may support stronger tracing and end-use monitoring while resisting excessive reporting obligations.

Potential tension: transparency versus commercial and security interests.

5. CONFLICT-AFFECTED AND FRAGILE STATES

Likely to prioritise:

- institutional capacity-building;
- border management;
- peacebuilding;
- DDR;
- weapons collection;
- and international financial and technical assistance.

These states may argue that international obligations must be accompanied by resources to implement them.

Potential tension: ambitious international standards versus limited state capacity.

6. SMALL AND VULNERABLE STATES

Likely to favour:

- multilateralism;
- sovereignty;
- predictable international rules;
- capacity-building;
- and protection from external coercion.

They may be particularly concerned that gray-zone competition between major powers can destabilise smaller states.

Potential tension: maintaining neutrality while responding to external pressure.

7. STATES WITH SIGNIFICANT MARITIME OR ISLAND TERRITORY

(Additional bloc for delegates in this agenda area)

Likely to prioritise:

- freedom of navigation;
- protection against paramilitary or "gray hull" coercion;
- clarity on the application of the law of the sea to gray-zone activity;
- and regional confidence-building measures.

Potential tension: asserting territorial claims versus avoiding escalatory naval incidents.

8. STATES WITH ADVANCED CYBER CAPABILITIES

(Additional bloc for delegates in this agenda area)

Likely to prioritise:

- voluntary norms over binding cyber treaties;
- flexibility to conduct intelligence and defensive cyber operations;
- and continued primacy of the GGE/OEWG processes over any new DISEC-created cyber body.

Potential tension: norm-setting versus capability retention.

6. GLOSSARY OF KEY TERMS

Attribution — The process of identifying the actor responsible for a given act, which may be technical, political, or legal in nature, and which does not automatically establish legal responsibility.

Chapter VII (UN Charter) — The section of the UN Charter granting the Security Council authority to take binding action, including sanctions and the use of force, in response to threats to international peace and security.

Diversion — The unauthorised redirection of legally produced or transferred arms to recipients or end-uses not authorised by the original transfer.

DDR (Disarmament, Demobilization and Reintegration) — A process supporting former combatants in laying down arms, leaving armed groups, and reintegrating into civilian life, often supported by UN peace operations.

End-Use Monitoring — Mechanisms used to verify that transferred arms are used by, and remain with, the authorised recipient.

Gray Zone Warfare — Strategic activity intended to advance political or security objectives while remaining below, around, or deliberately ambiguous in relation to the threshold of conventional armed conflict.

Hybrid Warfare — The coordinated use of military and non-military instruments (political, economic, informational, cyber) to pursue strategic objectives; overlaps with but is broader than the gray zone concept.

Non-State Armed Actor — An organised armed entity that is not formally part of the armed forces of a state.

Proxy Warfare — The use of, or support to, another actor by a state to pursue strategic objectives while maintaining a degree of separation from direct involvement.

Small Arms and Light Weapons (SALW) — Man-portable weapons such as pistols, rifles, machine guns, and light weapons systems, which are the primary focus of the Programme of Action.

Sanctions Regime — A set of coercive, non-military measures (asset freezes, travel bans, arms embargoes) imposed by the Security Council or individual states against a target state, entity, or individual.

Use of Force (Article 2(4)) — The general prohibition in the UN Charter against the threat or use of force against the territorial integrity or political independence of any state, subject to limited exceptions including self-defence under Article 51.

7. QUESTIONS A RESOLUTION MUST ANSWER

A good DISEC resolution should not simply condemn gray-zone warfare.

It should answer the following practical questions:

1. How should the international community distinguish gray-zone activity from ordinary diplomatic, economic or political competition?
2. Should the UN develop a common working definition of gray-zone activity, or would doing so risk creating an overly broad category?
3. How can states improve attribution of hostile activities without compromising legitimate intelligence or national-security information?
4. How can the international community prevent states from using non-state armed actors as instruments of strategic competition?
5. What mechanisms can reduce the diversion of legally transferred arms to unauthorised recipients?
6. How can the Programme of Action and International Tracing Instrument be implemented more effectively?
7. How can implementation of the Arms Trade Treaty complement existing UN frameworks?
8. How can developing and conflict-affected states receive technical and institutional assistance for arms management?
9. Should states strengthen international reporting concerning suspected diversion and illicit arms transfers?
10. How can regional organisations cooperate with the UN in monitoring illicit arms flows?
11. How can the international community address terrorist financing and other forms of support to armed groups while protecting legitimate humanitarian activity?
12. How can states prevent non-state actors from acquiring materials relevant to weapons of mass destruction?

13. How should emerging technologies be incorporated into existing international security frameworks?
 14. What role should sanctions, arms embargoes and other Security Council mechanisms play when armed groups threaten international peace and security?
 15. How can DISEC proposals complement rather than duplicate the mandates of the Security Council, UNODA, UNCTC, UNIDIR and regional organisations?
 16. What safeguards should exist against the misuse of "gray-zone warfare" as a justification for excessive intervention or restrictions on legitimate political activity?
 17. How can international responses prevent escalation while still creating credible deterrence?
 18. How can civilian protection remain central to international responses to non-state armed actors?
 19. What role should voluntary confidence-building measures (military-to-military hotlines, incident-reporting mechanisms) play in reducing the risk of miscalculation during gray-zone confrontations?
 20. Should DISEC recommend that Member States submit voluntary national reports on gray-zone-related risks alongside existing PoA and ATT reporting mechanisms, to avoid creating a wholly new reporting burden?
-

8. SAMPLE OPERATIVE CLAUSE BANK

The following clause starters are illustrative only, intended to help delegates draft precise, actionable language. They are not a finished resolution and should be adapted, combined, and made more specific during committee negotiation. Delegates should avoid copying clauses verbatim without tailoring them to their bloc's position.

On definitions and scope:

Encourages Member States and relevant UN bodies to develop a shared, non-exhaustive understanding of gray-zone activity for the purposes of information-sharing and early-warning cooperation, without prejudice to existing legal definitions of the use of force, armed attack, or armed conflict;

On attribution and transparency:

Calls upon Member States to consider voluntary, confidence-building measures — including incident-reporting channels and military-to-military communication mechanisms — to reduce the risk of miscalculation arising from ambiguous or unattributed hostile activity;

On arms diversion:

Urges Member States to strengthen national stockpile management, end-use verification, and marking and record-keeping practices consistent with the Programme of Action and the International Tracing Instrument, and *requests* UNODA to expand technical assistance programmes to states with limited institutional capacity;

On state sponsorship of non-state actors:

Reaffirms the obligations of Member States under Security Council Resolution 1540 to refrain from providing any form of support to non-state actors seeking to acquire weapons of mass destruction, and *encourages* enhanced national export-control and border-security cooperation to prevent exploitation of regulatory gaps;

On counter-terrorism financing:

Reiterates the importance of full implementation of Security Council Resolution 1373, including measures to counter terrorist financing, while *underscoring* the necessity of protecting principled, impartial humanitarian action from unintended restriction;

On cyber and emerging technology:

Welcomes the ongoing work of the Open-Ended Working Group on developments in the field of information and telecommunications and *encourages* Member States to implement the voluntary, non-binding norms of responsible state behaviour already agreed by consensus;

On regional cooperation:

Invites relevant regional and sub-regional organisations to strengthen information-sharing arrangements with UNODA and the Counter-Terrorism Committee Executive Directorate regarding cross-border movement of non-state armed actors and illicit arms flows;

On civilian protection:

Emphasizes that all measures adopted pursuant to this resolution must be implemented in a manner consistent with international humanitarian law and international human rights law, with particular attention to the protection of civilians and safeguarding of humanitarian access;

On institutional coordination:

Requests the Secretary-General to prepare a report examining opportunities to improve coordination among UNODA, the Counter-Terrorism Committee, the 1540 Committee, and relevant regional bodies in addressing the security challenges

posed by gray-zone activity and non-state armed actors, for consideration at a future session of the General Assembly.

9. COUNTRY RESEARCH CHECKLIST

Before committee, delegates should be able to answer the following about their assigned Member State:

Security environment

- Has the state experienced gray-zone activity directed against it (cyber intrusions, proxy conflict, economic coercion, disinformation, maritime incidents)?
- Has the state been accused of supporting, or does it maintain relationships with, any non-state armed actors abroad?
- Does the state face an active or recent internal or cross-border threat from non-state armed groups?

Legal and treaty commitments

- Is the state a party to the Arms Trade Treaty? Has it submitted required reports?
- Has the state endorsed the Programme of Action and International Tracing Instrument, and does it participate in Biennial Meetings of States?
- What is the state's record on implementing Security Council Resolutions 1373 and 1540 (e.g., national reports to the CTC and 1540 Committee)?

Institutional capacity

- Does the state have the institutional and technical capacity to implement stronger arms-tracing, stockpile-management, or border-security measures, or would it need international assistance?
- Has the state received or provided capacity-building assistance related to small arms control or counter-terrorism?

Alliances and blocs

- Which regional or political blocs does the state belong to, and what positions have those blocs historically taken on disarmament and counter-terrorism issues?
- Does the state have close allies whose positions it is likely to follow or diverge from on this agenda?

Technology and cyber posture

- Does the state have significant offensive or defensive cyber capabilities?

- Has the state been a victim of, or alleged perpetrator of, state-linked cyber operations?
- What has the state's position been in the UN GGE/OEWG cyber norms processes?

Domestic priorities

- What are the state's core red lines on sovereignty and non-interference?
- Would the state support new international reporting obligations, or would it view these as burdensome or intrusive?
- What specific, actionable proposal could this state credibly champion or co-sponsor in committee?

10. SUGGESTIONS FOR FURTHER READING

Delegates seeking to strengthen their position papers and speeches beyond this guide may wish to independently research:

- national position statements and voting records at recent Programme of Action Biennial Meetings of States;
- publicly available reports of UN Panels of Experts monitoring relevant Security Council sanctions regimes, for real-world examples of arms diversion and non-state actor financing;
- consensus reports of the UN Group of Governmental Experts and Open-Ended Working Group on cyber norms;
- their assigned state's national reports to the Counter-Terrorism Committee and the 1540 Committee;
- academic and think-tank literature on the "gray zone" and "hybrid warfare" concepts, bearing in mind that these are contested and evolving terms rather than settled doctrine;
- regional organisation statements on non-state armed actors and illicit arms flows relevant to their assigned state's region.

11. BIBLIOGRAPHY

United Nations General Assembly. First Committee — Disarmament and International Security. United Nations Office for Disarmament Affairs. Disarmament and Arms Control Resources. United Nations. Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects. United Nations. International Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons. United Nations. Arms Trade Treaty. United Nations Security Council. Resolution 1373 (2001) and Counter-Terrorism Committee Framework. United Nations Security Council. Resolution 1540 (2004) and Non-Proliferation of Weapons of Mass Destruction to Non-State

Actors. United Nations Security Council. Sanctions and Arms Embargo Framework. United Nations. Disarmament Week / Conventional Arms and Emerging Technologies Resources. United Nations. Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. United Nations. Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace. NATO. Hybrid Threats and Hybrid Warfare Reference Curriculum. UN First Committee — Disarmament and International Security First Committee — Resources First Committee — Official Documentation United Nations — Disarmament UN Disarmament Agenda UN Security Council — Sanctions Information UN Security Council — Sanctions and Other Committees Security Council Counter-Terrorism Committee — Mandate UN Security Council Resolution 1540 — Fact Sheet UN Peacekeeping — Disarmament, Demobilization and Reintegration International Committee of the Red Cross — International Humanitarian Law and Non-State Armed Groups Resources