CREDOMUN III



DISEC

STUDY GUIDE

LETTER FROM THE SECRETARY GENERAL

It is my team's and my utmost pleasure and honour to host you at the 3rd edition of CREDOMUN as the Secretary-General.

A few days from now, all of you will be walking through the doors of your committees, and while it may seem daunting now, trust me when I say this: it will be one of the most fulfilling experiences of your life.

The three days of the conference are not just about debate, drafting resolutions, or winning awards, but about experiencing something larger than yourself.

This edition of CREDOMUN gives you the platform to explore a wide range of cultures and engage with diverse schools of thought from across the city.

After being honoured with the role of DDG at last edition's conference, I am gratefully excited to host all of you amazing delegates this year as the Secretary-General. This places the utmost responsibility on my team to ensure that you leave this conference having gained something meaningful from it.

While I do not intend to bore you right now whilst you read this note, I must warn you about the time when I will have to give a speech in front of you. At that time, I will take no action to stop myself from being boring and annoying.

Till then, you have everything you could ever need in these study guides and all the time in the world before the eve of the 23rd. I look forward to seeing the ideas you challenge, the solutions you develop, and the memories you create throughout the conference.

Warm regards,

Fazl Abbas,
Secretary General,
Credo Model United Nations III

LETTER FROM THE PRESIDENT

Dear Delegates,
It is my humble privilege to welcome you all to the 3rd edition of CredoMUN

CredoMUN has been the focal point of my debating journey, from being a delegate in its 1st edition, then an ACD in its 2nd edition and now the President of the 3rd edition, CredoMUN has truly given me a platform to learn and lead

I have always skipped through the notes in a study guide because why spent time reading the note from someone i dont even know, so please do skip along if I am eating into your limited research time.

The reality is CredoaMUN is truly special because here, delegates can feel at home, debate and have fun, make memories without having to process 5 Bashes at the same time, because at CredoMUN every delegate gets a chance to express themselves, learn how to improve and make unforgettable memories along the way.

As the President of this conference, I promise you all one thing, excellence. Whether it is across exceptional debate, incredible committee topics, or the wonderful people you meet along the way, my team and i ensure that you will be part of the best CredoMUN to date

And if you ever feel overwhelmed by the spectacle, you can always find me practicing a long range volley in our futsal court

Warm Regards,

Saif Khan,
President,
Credo Model United Nations III

THE STRAIT OF ESCALATION

Preventing the Militarization of Maritime Chokepoints

TABLE OF CONTENTS

Introduction to the Committee 4
Overview 4
TOPIC: The Militarization of Maritime Chokepoints: Preventing the Proliferation of Drone and Missile Technology to Non-State Actors 5
Introduction to the Agenda 5
Background of the Agenda 6
Overview 6
Conventional Deterrence and the Legacy of State-Centric Blockades 7
The Era of Low-Tech Piracy and Asymmetric Security Gaps 7
The Democratization of Precision Flight and Dual-Use Leakage 8
Agenda Breakdown 8
The Proliferation Loophole and Asymmetric Sourcing 9
The Legal Vacuum of Sovereignty vs. Interdiction 9
The Attribution Deficit 9
Technical Profile of Asymmetric Maritime Weapons 9
Uncrewed Aerial Systems (UAS) & Loitering Munitions 10
One-Way Attack (OWA) Long-Range Loitering Munitions 10
Modified Hobbyist Quadcopters & Hexacopters 10
Militarization of Consumer-Grade Components 10
Uncrewed Surface Vessels (USVs) & Loitering Torpedoes 10
Explosive-Laden Remote-Controlled Boats 10
Loitering Torpedoes & Semi-Submersible Crafts 11
Targeting and Communication Mechanics 11
Anti-Ship Cruise Missiles (ASCMs) & Shore-to-Sea Ballistic Weapons 11
Mobile Transporter-Erector-Launchers (TELs) 11
Decentralized Radar Targeting Frames 11
Terminal Guidance and Kinetic Trajectories 12
Supply Chain Mechanics & The Logistics of Proliferation 12
The Anatomy of a Completely Knocked-Down (CKD)Kit 12
Airframe and Hull Concealment 12
Propulsion Subsystems 13
Guidance Electronics and Actuators 13
The Transnational Smuggling Funnel 13
The Layering of Front Companies 13
Exploitation of Neutral Transshipment Ports 13
Maritime "Ghost Fleets" and Ship-to-Ship (STS) Transfers 14

AIS Deactivation 14
Ship-to-Ship (STS) Transfers 14
Beachhead Infiltration 14
Financial Architectures of Proliferation **14**
The Asymmetric Financing Loop 14
Illicit Local Taxation Regimes 14
Smuggling of High-Value Natural Resources 15
Anonymized Cryptocurrency Capital Channels 15
The Hawala Informal Value Transfer System 15
State-Proxy Financial Channels 15
The Role of Aerospace and Tech MNCs **14**
Existing International Frameworks and Their Gaps **15**
United Nations Convention on the Law of the Sea (UNCLOS) 1982 16
The Missile Technology Control Regime (MTCR) 17
UN Security Council Resolution 1540 (2004) 17
Targeted UN Arms Embargoes 18
Key Challenges to International Security and Non-Proliferation **21**
Tracking Vulnerabilities and the Dual-Use Procurement Loophole 21
The Legal Vacuum of Sovereignty vs. Active Maritime Interdiction Protocols 22
The Attribution Deficit and Asymmetric State Sponsorship 23
Case Studies **24**
1) The Bab al-Mandeb Strait and the Red Sea Crisis 24
2) The Strait of Hormuz 25
3) The Strait of Malacca 25
4) The Suez Canal 25
National Perspectives **26**
1) United States of America 26
2) Islamic Republic of Iran 26
3) Kingdom of Saudi Arabia 27
4) Republic of Singapore 27
5) Arab Republic of Egypt 28
Questions Any Resolution Must Answer (QARMA) **30**
References **31**

Introduction to the Committee

The First Committee of the United Nations General Assembly (DISEC) is tasked with evaluating global vulnerabilities, transnational security hazards, and disarmament challenges that jeopardize international stability. Operating in direct alignment with the United Nations Office for Disarmament Affairs (UNODA), DISEC crafts comprehensive multilateral frameworks to counter aggression and strengthen global peace regimes.

Overview

The structural operations of DISEC follow a systematic, threefold progression: General Debate, Thematic Discussions, and Action on Drafts. The committee will debate specific, targeted situations, address the challenges they present, and submit a draft resolution at the conclusion of the session. The committee then votes on and adopts draft resolutions containing strategic recommendations for the international community.

Grounded in the core objectives of the UN Charter, DISEC's primary focus is to de-escalate geopolitical friction, promote uniform arms reduction, and lead conflict-prevention strategies on a global scale.
As a General Assembly body, DISEC cannot adopt binding measures or impose sanctions; its resolutions are recommendations to member states and, where relevant, to the Security Council.

Areas of Focus

Global Disarmament: Eliminating the systematic advancement and increase of chemical, biological, radiological, and nuclear weapons, alongside stockpiles of conventional arms and small weaponry.

Arms Control Mechanics: Designing restrictive frameworks to manage the international transfer of sensitive hardware and dual-use systems that risk destabilizing fragile territories.

Non-Proliferation Regimes: Strengthening treaty compliance, fostering international legal collaboration, and blocking the illicit migration of mass-destruction technologies.

Conflict Prevention Protocols: Isolating and mitigating the underlying political, economic, and territorial catalysts of disputes before they boil over into cross-border crises.

Regional Demilitarization & Verification: Establishing multilateral frameworks to limit military build-ups in sensitive maritime corridors, defining localized weapon-free zones, and designing technical monitoring mechanisms to verify disarmament compliance.

Unconventional & Emerging Threats: Continuously adapting to counter contemporary military security dilemmas, including automated cyber warfare, asymmetric terror syndicates, and emerging weapons technologies

TOPIC: The Militarization of Maritime Chokepoints: Preventing the Proliferation of Drone and Missile Technology to Non-State Actors

Introduction to the Agenda

More than 80% of the volume of global trade in goods is carried by sea and depends heavily on narrow transit corridors known as maritime chokepoints. Strategic waterways—including the Bab al-Mandab Strait, the Strait of Hormuz, the Suez Canal, and the Strait of Malacca—serve as the economic lifeblood of the global supply chain, channeling vital food, manufacturing inputs, and energy supplies. In 2024, oil flows through the Strait of Hormuz were equivalent to approximately 20% of global petroleum-liquids consumption. Historically, keeping these straits safe and ensuring freedom of navigation was a matter of state-on-state conventional deterrence, managed by sovereign state navies deploying large-scale warships.

However, rapid technological shifts have completely altered this conventional security dynamic. The democratization and cheap manufacturing of Uncrewed aerial systems (UAS), remote-controlled explosive boats, and Anti-Ship Cruise Missiles (ASCMs) have given non-state actors precision strike capabilities. By setting up land-based anti-access/area denial (A2/AD) zones right along the coastlines of critical straits, insurgent proxy networks can hold international trade hostage and bypass conventional naval power at almost no cost. Because these systems are frequently smuggled as disassembled civilian dual-use parts, they easily slip past standard customs borders and traditional arms embargoes.

For the Disarmament and International Security Committee (DISEC), this agenda demands a deep dive into global tracking vulnerabilities, export controls, and international security gaps. Delegates must create new legal and practical frameworks to sever the supply chains feeding armed groups and their state sponsors, because attacks on shipping have already caused severe disruption to global trade and energy markets. Commercial traffic through the Strait of Hormuz fell by more than 90 percent after the 2026 Iran war began, producing a global fuel crisis.

This modern security crisis exposes a fundamental contradiction between international maritime law, trade liberty, and asymmetric security realities that traditional state-centric treaties cannot bridge. The existing international framework assumes that threats to shipping come from easily identifiable state militaries subject to international law. In stark contrast, modern non-state actors use decentralized, transnational networks to convert ordinary consumer technologies into lethal weaponry. This leaves the international community without a clear blueprint for response.

Delegates should note that legacy frameworks require critical reassessment and reform to address these modern gaps. The committee faces the challenge of adapting existing non-proliferation agreements originally designed for finished military hardware, so that they can better account for the cross-border flow of dual-use components without disrupting civilian commercial innovation. Furthermore, there is a growing recognition that traditional naval patrols alone may no longer be sufficient against land-to-sea asymmetric strikes. Resolutions should therefore explore ways to modernize shipping security protocols, strengthen current maritime treaties, and foster robust regional intelligence-sharing networks under the DISEC mandate to proactively disrupt illicit supply networks before they destabilize strategic chokepoints, ranging from high-intensity conflict zones in the Red Sea to highly trafficked commercial channels like the Strait of Malacca.

Background of the Agenda

Overview

The strategic fragility of maritime bottlenecks is a long-standing geopolitical vulnerability rather than a sudden byproduct of the drone era. Historically, international shipping lanes have been bounded by geographic bottlenecks where regional frictions, territorial disputes, and weak domestic state structures frequently intersect. Whether examining the vital energy lanes of the Strait of Hormuz, the dense trade corridors of Southeast Asia, or the highly contested waters of the Black Sea maritime gateways— controlling or securing these narrow shipping passages depended entirely on the deployment of massive, capital-intensive state navies capable of enforcing conventional fleet-on-fleet deterrence. Disrupting trade on a global scale required industrial shipyard capabilities, meaning that non-state maritime interference was historically limited to low-tech, localized piracy or opportunistic sabotage. Modern military innovations have not created these underlying regional rivalries; rather, they have reshaped the physical constraints of the coastline, offering irregular factions the mechanism to project lethal, precision force across vast maritime distances with a high degree of operational deniability.

Concurrently, the global commercial market has decentralized the production of high-tech components, allowing insurgent forces to acquire highly effective anti-access/area-denial (A2/AD) capabilities without the need for massive sovereign military infrastructure. This shift presents a profound geopolitical contradiction: while technological access has democratized tactical defense options for smaller actors contesting regional powers, it has simultaneously exposed global supply chains to unprecedented trade extortion, soaring insurance premiums, and systemic economic blockades. Evaluating this agenda thoroughly requires delegates to trace how historical territorial flashpoints, international maritime trade routes, dual-use commercial shipping networks, and uncrewed autonomous systems have converged to form the modern crisis of chokepoint militarization.

Conventional Deterrence and the Legacy of State-Centric Blockades

Pre-2000s Era

Before the turn of the century, the defense of maritime chokepoints was viewed strictly through the lens of conventional, state-on-state military strategy. During the Cold War and its immediate aftermath, threats to strategic waterways—such as the Strait of Hormuz or the Bab al-Mandab—consisted of formal naval blockades, state-deployed sea mines, or fleet-on-fleet engagements. International security frameworks assumed that only sovereign nations possessed the massive industrial, logistical, and financial capital required to disrupt global shipping lanes or deny access to a naval force.

International efforts slowly laid the legal and operational groundwork to help address these conventional maritime hazards. The United Nations Convention on the Law of the Sea (UNCLOS), adopted on 10 December 1982, established universal maritime zones and codified the right of Transit Passage through international straits, which coastal states may not suspend, to prevent arbitrary lockouts. Concurrently, informal state-to-state export oversight groups, such as the Missile Technology Control Regime (MTCR) in 1987, were created to prevent rogue states from acquiring heavy ballistic missile hardware. These early mechanisms were tailored entirely around visible, state-owned military vessels and completed weapons arrays, assuming that state accountability and conventional deterrence would be enough to keep the seas open.

The Era of Low-Tech Piracy and Asymmetric Security Gaps

2000s–2009

The rapid expansion of global shipping volume in the 2000s exposed strategic waterways to a different type of disruption: non-state maritime piracy, most notably originating from the porous, unmonitored coastlines of Somalia. Operating out of collapsed state environments, pirate networks used low-tech equipment, such as fiberglass skiffs, ladders, and basic small arms like AK-47s and RPGs, to board and hijack commercial container ships for multi-million-dollar ransoms. These actors did not seek to destroy vessels or wage ideological wars; instead, they exploited the vast, open space of the sea for financial extortion, proving that under-defended merchant vessels could be easily compromised by non-state actors.

The international community responded by mobilizing collaborative naval task forces, such as Combined Task Force 151, and passing a series of UN Security Council resolutions authorizing foreign navies to enter territorial waters to suppress piracy. During this same window, UN Security Council Resolution 1540 (2004) legally bound states to implement strict domestic border and export controls to stop non-state actors from acquiring weapons of mass destruction. Yet, the rapid growth of these security frameworks outpaced the development of laws tracking sub-military technology. Because piracy was viewed strictly as a criminal, low-tech law enforcement problem over water, international law left a critical gap: it failed to anticipate that non-state factions would eventually migrate their launch pads deep onto land and adopt precision military technology.

The Democratization of Precision Flight and Dual-Use Leakage

2010s–Present

The mid-2010s marked a major technological pivot point as advanced guidance systems, satellite navigation modules, and drone technologies slipped out of exclusive military monopolies and flooded the commercial civilian market. The rapid growth of commercial tech industries led to the mass production of cheap, high-performance unmanned aerial vehicles (UAVs) for agricultural tracking, filmmaking, and industrial logistics. For the first time, complex flight software, stabilization gyroscopes, and composite carbon-fiber components became universally accessible online to anyone with a credit card, completely bypassing the oversight of traditional military arms trade manifests.

This technological democratization allowed non-state actors to leapfrog decades of conventional naval development. Factions operating along strategic coastlines began systematically importing these commercial, dual-use parts, using neutral shell companies and porous maritime transshipment hubs. Once inside insurgent territories, these commercial components were combined with modular blueprints to construct long-range loitering munitions, remote-controlled explosive boats, and land-to-sea cruise missiles. This transformation effectively turned irregular militias into state-equivalent littoral missile forces, rendering old-school naval border enforcement and standard customs manifests obsolete, while setting the stage for the modern crisis of chokepoint militarization.

Agenda Breakdown

The crisis of chokepoint militarization expands into three fundamental structural challenges that the international community has struggled to reconcile.

The Proliferation Loophole and Asymmetric Sourcing

Traditional non-proliferation treaties were designed to monitor the movements of state militaries purchasing completed, recognizable weapon systems. Non-state actors completely bypass these mechanisms by using decentralized proxy networks to import commercial engines, composite fibers, carbon tubing, and consumer electronics across neutral borders. Once inside militia territory, engineers assemble precision-guided loitering munitions or water-borne explosive drones using basic blueprints. This systemic circumvention allows asymmetric actors to wield strategic military influence at a fraction of the cost of a state navy, crippling commercial freedom of navigation without triggering conventional arms tracking indicators.

The Legal Vacuum of Sovereignty vs. Interdiction

The primary legal battleground centers on the jurisdiction of international waters versus sovereign territory. Under UNCLOS, foreign navies and merchant vessels enjoy the freedom of navigation on the high seas and the right of transit passage through international straits. Some naval powers, most notably the United States, also conduct Freedom of Navigation Operations (FONOPs), which are operational programs that challenge maritime claims a state considers excessive. FONOPs are a policy tool, not a legal doctrine.
However, the legal authority of foreign navies to intercept, board, and search civilian vessels suspected of smuggling components inside a coastal state’s Exclusive Economic Zone (EEZ) is highly ambiguous. Furthermore, because launch sites are frequently embedded within civilian infrastructure on land, naval coalitions face a severe operational paradox. Striking a launch site on another state’s territory is generally prohibited by Article 2(4) of the UN Charter, which bars the use of force against other states. Such a strike is lawful only in three cases: when the Security Council authorizes it, when the host state consents, or when it is justified as self-defense under Article 51. States disagree sharply over whether self-defense applies to attacks launched by non-state groups from another country’s soil.

The Attribution Deficit

Drones and uncrewed vessels have detached the concept of kinetic warfare from clear military accountability. When a proxy network launches an attack at a commercial vessel, the state sponsor providing the underlying technology and radar targeting data maintains plausible deniability. Without ironclad forensic evidence linking a specific state to an incident, the international community faces immense difficulty coordinating formal accountability measures or recommending UN sanctions, leading to legislative paralysis while strategic shipping lanes remain compromised.

Technical Profile of Asymmetric Maritime Weapons

The modern tactical crisis at international maritime chokepoints is driven by the weaponization of low-cost, commercial technologies. Non-state actors have successfully bypassed conventional navies by deploying asymmetric systems that match the precision strike capabilities of sovereign states at a fraction of the cost. These systems are split into two primary technological classes: uncrewed aerial vehicles that exploit open-market electronics and remote-controlled surface vessels configured for waterline detonations.

Uncrewed Aerial Systems (UAS) & Loitering Munitions

Non-state militias use a tiered array of uncrewed aerial platforms to overwhelm the multi-layered air defense systems of modern naval vessels. These platforms are categorized by their design, range, and modification methods.

One-Way Attack (OWA) Long-Range Loitering Munitions

Long-range loitering munitions function as low-cost cruise missiles, using simple plywood or composite hulls to reduce their radar visibility. They are powered by generic, commercial two-stroke internal combustion engines originally designed for model aircraft or industrial lawnmowers. Flying at low altitudes to escape radar detection, these platforms can travel over 1,000 kilometres before diving directly into a target ship's superstructure.

Modified Hobbyist Quadcopters & Hexacopters

For short-range tactical strikes, militias modify commercial off-the-shelf agricultural or racing drones, equipping them with simple mechanical hooks to drop modified mortar rounds or anti-tank grenades directly onto undefended merchant vessels. They hover directly over commercial vessels to target bridge windows, deck-mounted cargo containers, or crew quarters.

Militarization of Consumer-Grade Components

Non-state actors innovate by converting everyday civilian electronics into military guidance systems. To bypass naval electronic jamming, militias connect standard commercial GPS units to multiple satellite networks, integrate Inertial Measurement Units utilizing basic dead-reckoning algorithms to maintain flight paths, and upload open-source autopilot software onto commercial microchips to grant autonomous navigation capabilities. Lastly, low-cost first-person view cameras and transmitters provide terminal guidance, allowing land-based operators to steer drones into vulnerable ship structures in real time.

Uncrewed Surface Vessels (USVs) & Loitering Torpedoes

Surface-level threats have shifted from traditional pirate skiffs to low-profile, uncrewed maritime vessels that carry heavy explosive payloads directly to a ship's waterline:

Explosive-Laden Remote-Controlled Boats

Militias use V-shaped fiberglass hulls, similar to recreational speedboats, to minimize radar visibility amid ocean waves. These boats are stripped of manual controls to accommodate large fuel bladders and heavy explosive charges weighing between 250 to 500 kilograms, using high-horsepower commercial marine engines to outmanoeuvre heavy naval vessels.

Loitering Torpedoes & Semi-Submersible Crafts

To bypass visual lookouts and deck-mounted machine guns, militias build low-profile semi-submersible hulls that cruise just centimetres below the water's surface. These platforms act as low-cost loitering torpedoes, running quietly on battery-powered electric motors to target a ship's vulnerable rudder or propeller arrays to immobilize it.

Targeting and Communication Mechanics

These vessels utilize mounted commercial satellite internet terminals covered in radar-absorbent resin, allowing land-based operators located hundreds of kilometres away to stream live video feeds and steer them over the horizon. While high-end naval USVs use military LIDAR, non-state variants rely on commercial marine navigation radars and thermal cameras to identify shipping silhouettes through fog, darkness, or heavy sea spray. Mechanical impact switches made from repurposed industrial machinery are fitted to the nose of the hull to ensure the payload detonates instantly upon contact.

Anti-Ship Cruise Missiles (ASCMs) & Shore-to-Sea Ballistic Weapons

Beyond uncrewed platforms, non-state groups possess heavy shore-to-sea missile capabilities, creating land-based anti-access/area-denial (A2/AD) zones alongside critical international straits.

Mobile Transporter-Erector-Launchers (TELs)

Factions avoid retaliatory air strikes by mounting anti-ship cruise missiles onto commercial flatbed trucks or modified cargo transport vehicles. These vehicles remain hidden inside inland tunnels, agricultural warehouses, or civilian urban areas. They drive to the rugged coastline, erect the launch container, fire the weapon, and relocate within minutes, rendering pre-planned counter-battery strikes ineffective.

Decentralized Radar Targeting Frames

Operating high-powered maritime surveillance radars constantly makes them easy targets for naval anti-radiation missiles. Non-state actors counter this by installing commercial Automatic Identification System (AIS) monitoring stations and electronic intelligence (ELINT) antennas along high ground to track merchant ships without emitting radio signals. Coastal surveillance radars are powered on for brief intervals, often less than 60 seconds, to capture high-accuracy speed and distance coordinates for target vessels before shutting down to evade electronic detection.

Terminal Guidance and Kinetic Trajectories

Once launched, the missiles use solid-fuel boosters and micro-turbojets to drop to low altitudes just metres above the water's surface, sliding completely under naval radar curtains. During the final phase of flight, the missile activates an internal active radar seeker or an infrared camera to lock onto the largest metallic mass on the horizon, ensuring a high-impact strike against merchant ship hulls.

Delegates should recognize that the highly mobile and commercially derived nature of these weapons profiles creates an unsustainable security dynamic for traditional naval forces.

When non-state actors can deploy low-cost loitering munitions and hidden coastal batteries to hold international shipping lanes hostage, purely kinetic, defensive naval responses become economically and operationally exhausting. The committee should note that traditional maritime security mechanisms lack clear protocols for counteracting land-based, decentralized targeting frames that exploit civilian infrastructure. Therefore, delegates must look beyond standard defensive military maneuvers and evaluate how international frameworks can be modernized to address the technical availability of these weapon systems at their structural source.

Supply Chain Mechanics & The Logistics of Proliferation

Irregular militias rarely have the heavy factories needed to manufacture complex weapons from scratch. Instead, their military strength depends on buying normal commercial products from around the world and smuggling them into their territories.

The Anatomy of a Completely Knocked-Down (CKD) Kit

To bypass the United Nations Register of Conventional Arms (UNROCA) and standard customs security checks, state sponsors disassemble advanced weaponry into Completely Knocked-Down (CKD) kits. These kits split a weapon into individual components that resemble civilian industrial goods, categorizing them under harmless Harmonized System (HS) customs codes.

Airframe and Hull Concealment

The structural bodies of anti-ship cruise missiles or loitering drones are manufactured in modular, bolt-together segments, allowing hulls to be labeled on customs forms as fiberglass industrial water pipes, carbon-fiber wind turbine parts, or agricultural drainage tubes.

Propulsion Subsystems

Liquid-fuel micro-turbojet engines are disassembled into rotors, injectors, and fuel pumps to be shipped alongside commercial truck engine parts, while one-way attack drones use two-stroke internal combustion engines that pass through customs labeled as commercial lawnmower engines or water-well generators

Guidance Electronics and Actuators

Guidance units are stripped of all military markings, mixing flight control microchips into large shipments of consumer electronics or remote-controlled toy parts while high-torque electric servo motors used to move missile steering fins are imported under the guise of factory automation gear.

Delegates may wish to explore new international tracing and verification frameworks specifically designed to monitor the cross-border flow of sensitive dual-use commercial components. While precedents exist for tracking conventional firearms and ammunition under existing United Nations (UN) frameworks, applying similar marking or verification standards to commercial electronics and industrial engines introduces significant regulatory challenges regarding compliance costs and manufacturing burdens.

Consequently, the committee should evaluate whether future resolutions should focus on physical component tracking mechanisms, or if delegates should instead pivot toward developing non-physical forensic tracking methods and state-to-state information-sharing protocols to disrupt illicit supply lines.

The Transnational Smuggling Funnel

Moving Completely Knocked-Down (CKD) kits from manufacturing facilities to coastal launch sites relies on multi-layered logistics networks. These operations intentionally obscure the country of origin and break the chain of legal custody through specific tactical stages:

The Layering of Front Companies

Smuggling networks establish dummy corporations across neutral jurisdictions, operating shell companies that exist only on paper and alter their legal names frequently to purchase dual-use electronic components from global manufacturers under the guise of local civilian infrastructure projects before exporting the hardware to secondary transshipment hubs.

Exploitation of Neutral Transshipment Ports

Smuggling operations avoid shipping cargo directly from a state sponsor to a militia-controlled destination. Instead, containers are routed through high-volume global transit hubs where logistics agents swap shipping containers and falsify manifest paperwork within free-trade zones, a process that strips the original manufacturer documentation and makes illicit cargo look like routine commercial shipments from neutral nations.

Maritime "Ghost Fleets" and Ship-to-Ship (STS) Transfers

The final delivery phase utilizes an unflagged ghost fleet of commercial and fishing vessels to complete the supply pipeline.

AIS Deactivation

Vessels may deactivate their mandatory Automatic Identification System (AIS) tracking transponders upon entering specific maritime zones, reducing their visibility on international satellite tracking systems.

Ship-to-Ship (STS) Transfers

Ghost fleet vessels rendezvous in unmonitored international waters under cover of darkness. High-value missile components and drone kits are transferred from large international container ships onto smaller civilian fishing dhows.

Beachhead Infiltration

These low-profile fishing vessels are often selected for their ability to blend in with local civilian maritime traffic. By utilizing alternative landing points along coastlines or inlets, such operations attempt to circumvent standard port security protocols and customs inspections.

Financial Architectures of Proliferation

To maintain transshipment pipelines and operate assembly facilities, non-state actors require sophisticated capital networks. These networks run on a dual-track financial framework: an Asymmetric Financing Loop that bypasses formal banking, and State-Proxy Financial Channels that abuse legitimate international commercial systems.

The Asymmetric Financing Loop

Non-state armed groups construct independent economic ecosystems to evade international financial scrutiny. These mechanisms operate entirely outside the oversight of central banks and global regulators:

Illicit Local Taxation Regimes

Factions occupying coastal territories enforce coercive extortion frameworks, levying mandatory customs duties on commercial transit vehicles at inland checkpoints and extracting regular licensing fees from local merchant associations to generate immediate operational liquidity.

Smuggling of High-Value Natural Resources

Militias systematically seize domestic state assets to exploit commodities. This includes the illicit extraction of crude oil, artisanal gold mining, and the unregulated trade of agricultural goods on regional black markets to secure untraceable cash reserves

Anonymized Cryptocurrency Capital Channels

Procurement networks leverage the digital asset ecosystem to bypass the Society for Worldwide Interbank Financial Telecommunication (SWIFT) banking system. They utilize privacy-focused cryptocurrencies on decentralized, unverified peer-to-peer (P2P) exchanges to purchase sensitive guidance software and tracking electronics from foreign vendors.

The Hawala Informal Value Transfer System

The primary mechanism for cross-border capital migration relies on traditional trust brokers, known as Hawaladars. This informal network transfers monetary value across jurisdictions without moving physical cash or utilizing electronic bank wires. First, a militia buyer in a coastal zone pays physical cash to a local broker. That local broker then contacts a secondary broker located in a foreign tech hub and relays an encrypted token. Finally, the foreign broker hands matching cash directly to the procurement agent abroad. The financial balances between the brokers are settled later through physical gold shipments or falsified trade invoices, leaving zero paper trails for anti-money laundering task forces to track.

State-Proxy Financial Channels

When direct financial support carries too much geopolitical risk, state sponsors exploit legitimate civilian economic infrastructure to hide their investments in proxy militias.

Humanitarian and Civilian Charity Fronts: Sovereign sponsors disguise capital transfers by routing funds through registered non-governmental organizations (NGOs) or religious endowments. These entities transfer capital into volatile zones under the guise of funding medical infrastructure or emergency food distribution, where local managers divert a percentage directly to militia weapon procurement offices.

Diversion of State Infrastructure Grants: Foreign sponsors provide direct development aid to weak host states via public works grants. These funds are designated for commercial port expansions, coastal highway networks, or electrical grid construction. Contracts are systematically steered toward front companies controlled by the militia, allowing them to utilize civilian development funds to build reinforced concrete military bunkers and underground assembly facilities.

Dual-Use Commercial Subsidies: State sponsors provide aggressive financial subsidies, tax exemptions, and low-interest loans to domestic commercial technology companies manufacturing civilian electronics. These firms intentionally overproduce hardware, such as commercial satellite modems or internal combustion engines, and export the surplus at artificial financial losses to front companies operated by the militia.

Exploitation of Diplomatic Immunities: Finally, high-value financial tools, encrypted communication hardware, and compact electronics are frequently moved across borders inside official diplomatic pouches. Under Article 27 of the Vienna Convention on Diplomatic Relations, these pouches are legally exempt from customs inspection and seizure, providing a secure method for delivering critical hardware directly to embassies located near militia command hubs.

The Role of Aerospace and Tech MNCs

The pivot of the contemporary maritime security agenda expands the definition of non-state actors to investigate the regulatory responsibilities of private multinational corporations (MNCs). The ultimate source of asymmetric weapon proliferation does not originate in dark smuggling caves, but within the commercial consumer supply chains of massive, multi-billion dollar technology manufacturers and civilian electronics hardware components. Commercial technology firms control the underlying proprietary technology that drives modern precision warfare, and this corporate ecosystem intersects with the maritime chokepoint crisis across three volatile dimensions.

The first dimension centers on the commercial satellite internet monopoly. Modern uncrewed surface vessels (USVs) and drone swarms require over-the-horizon, low-latency data streaming to hit fast-moving merchant ships inside chokepoints. This tracking capability relies heavily on commercial Low Earth Orbit (LEO) mega-constellations operated by private tech companies, such as the Starlink network operated by SpaceX. Because these satellite networks are privately owned, hostile non-state actors can purchase consumer-grade terminals through secondary shell companies, allowing unauthorized users to exploit neutral civilian data networks to steer lethal explosive boats into naval hulls. This operational landscape leaves corporate actors caught between global commercial expansion and active international security enforcement.

The second dimension involves the decentralization of high-end proprietary subsystems. Mass-market commercial microchips, structural carbon fibers, and compact electric actuators are widely manufactured for global consumer markets. However, through aggressive corporate sub-contracting, outsourcing, and extended globalized fulfillment networks, these proprietary dual-use parts inevitably leak into the open market. Shifting the agenda to include these commercial entities allows the committee to investigate how corporate actors can be held legally accountable for tracking their hardware downstream, ensuring that finished commercial products are not harvested by illicit procurement networks.
The third dimension is defined by the sovereign procurement loophole. Because private tech giants operate primarily on commercial profit motives, they aggressively market dual-use software algorithms, such as automated object recognition and terrain-mapping flight paths, to foreign governments and civilian tech hubs. Once exported via digital transfers under standard civilian licenses, these proprietary software packages are easily repurposed and uploaded onto asymmetric loitering munitions. The committee must determine how to implement binding end-user tracking mandates on corporate entities without crippling civilian commercial innovation and international trade liberties.

Existing International Frameworks and Their Gaps

International security, maritime law, and non-proliferation are governed through several independent legal treaties, arms control regimes, and maritime safety agreements. Collectively, these frameworks recognize the rights of sovereign states to freedom of navigation, secure commercial transit, and protection from illicit arms trafficking. However, each framework was developed independently, at different times, and for vastly different geopolitical reasons, meaning no single international framework comprehensively regulates the cross-border flow of commercial dual-use components, maritime interdiction boundaries, or asymmetric weapons operated by non-state actors.

United Nations Convention on the Law of the Sea (UNCLOS) 1982

The United Nations Convention on the Law of the Sea (UNCLOS) establishes the overarching legal framework for all maritime activities, balancing the coastal state's sovereignty with the global community's right to navigation. Specifically, Articles 37–44 dictate the rules of Transit Passage through straits used for international navigation, guaranteeing that foreign vessels and aircraft enjoy continuous and expeditious transit that cannot be suspended or impeded by littoral states. UNCLOS is a widely ratified treaty, legally binding on its states parties, that sets territorial limits, defines exclusive economic zones (EEZs), and governs the high seas. However, this convention was negotiated long before the development of contemporary autonomous weapons systems, loitering munitions, and remote-controlled explosive vessels. Because it relies heavily on traditional definitions of military vessels, it does not directly address the legal classification or regulation of uncrewed aerial systems (UAS) and uncrewed surface vessels (USVs) operating within strategic straits. Furthermore, UNCLOS holds sovereign flag states responsible for monitoring their own ships, meaning it fails to create binding, proactive interdiction mechanisms for foreign navies trying to intercept civilian vessels suspected of smuggling dual-use commercial components inside another state's EEZ. It also does not establish standardized criteria for maritime forensic evidence, satellite telemetry verification, or cross-border signal intelligence sharing needed to counter proxy-backed littoral attacks. UNCLOS is binding only on its state parties. The United States has not ratified it, though it states that it follows the Convention’s navigation provisions as customary international law. Iran signed in 1982 but never ratified, and it disputes that the transit passage regime reflects customary law that binds non-parties. This divergence is central to the Strait of Hormuz, where the legal status of transit passage is itself contested between Iran and the maritime powers.

The Missile Technology Control Regime (MTCR)

The Missile Technology Control Regime (MTCR) is an informal, voluntary political understanding established in 1987 and currently comprising 35 partners seeking to limit the proliferation of missiles, complete rocket systems, and unmanned aerial vehicles (UAVs). Specifically, its guidelines focus on systems capable of delivering weapons of mass destruction (WMD). Category I items, which face a strong presumption of denial, include complete rocket and uncrewed aerial systems capable of carrying a payload of at least 500 kg to a range of at least 300 km. Category II items, which receive case-by-case scrutiny, include complete UAVs capable of a range of at least 300 km regardless of payload, along with many related components such as certain small turbojet engines and navigation and avionics equipment. The MTCR operates via a common export control list (the Equipment, Software, and Technology Annex) implemented through each Partner’s national legislation to prevent destabilizing technology transfers. However, the MTCR is a non-binding political arrangement rather than a legally binding international treaty, meaning it relies entirely on voluntary national enforcement and lacks any formal dispute resolution or penalty mechanisms for non-compliance. Additionally, this framework was designed around traditional cold-war ballistic missile technologies. Although its Category II controls cover longer-range UAVs and some engines and avionics, it only partly regulates the contemporary flow of low-cost, commercial drone components, consumer electronics, and miniature engines. Short-range quadcopters, generic electronics and general-purpose engines generally fall below its range and performance thresholds, so proxy networks can import them as assembly parts, often by misdeclaring them or diverting them from legitimate buyers. The regime also does not establish any binding obligations on non-member states—many of whom are primary transit hubs or littoral hosts for non-state militias—nor does it provide mechanisms for real-time tracking of software algorithms and digital guidance telemetry across borders.

UN Security Council Resolution 1540 (2004)

UN Security Council Resolution 1540 (2004) is a landmark international mandate adopted under Chapter VII of the United Nations Charter, making it legally binding on all UN member states. Specifically, it requires all states to develop and enforce appropriate legal and regulatory measures against the proliferation of nuclear, chemical, and biological weapons and their means of delivery, with a specific focus on preventing non-state actors from acquiring such capabilities. The resolution obligates governments to establish domestic controls over related dual-use materials, implement effective border and export controls, and secure financial and physical logistics to stop illicit trafficking by unauthorized or terrorist groups.

However, the primary limitation of UNSCR 1540 in this context is its strict historical anchoring to Weapons of Mass Destruction (WMD) and heavy delivery systems. While it targets non-state actors legally, its language regarding "means of delivery" is interpreted by most states as applying to ballistic and cruise missiles designed for WMD payloads, rather than conventional, low-cost commercial drones, uncrewed surface vessels (USVs), or standard missile components used in asymmetric maritime harassment. Furthermore, the framework relies entirely on national self-reporting to the UN 1540 Committee rather than providing an active, international inspection or boarding force. It lacks specific standards for monitoring global containerized shipping manifests, commercial electronics, or dual-use software supply chains moving through international maritime chokepoints.

Targeted UN Arms Embargoes

Targeted UN Arms Embargoes, such as those historically established under UN Security Council Resolution 2216 (Yemen), alongside active mandates under Resolution 1970 (Libya) and Resolutions 733 (1992) and 2662 (2022) concerning Somalia, provide the primary structural templates concerning the immediate interdiction of weapons flowing to destabilizing non-state groups. They call for a total cessation of the supply, sale, or transfer of arms, military vehicles, and technical assistance to specified insurgent leaders and entities. These mandates also recognize the responsibilities of adjacent governments, regional naval coalitions, and international port authorities in making maritime chokepoints safer by actively monitoring trade lanes and inspecting high-risk cargo vessels suspected of carrying prohibited materials.

Nevertheless, targeted arms embargoes are geographically isolated crisis interventions rather than globally unified rules. The recent expiration and non-renewal of the targeted UN arms embargo on Yemen underscores the instability of these mechanisms, exposing a severe contemporary enforcement gap in critical corridors like the Bab al-Mandab Strait. These resolutions do not create a standardized international enforcement body, uniform maritime-liability standards for commercial shipping companies, or guaranteed legal remedies to penalize private suppliers. States also continue to use completely different definitions of what constitutes a restricted military item versus an unlisted commercial dual-use component, making international data collection, real-time evidence-sharing, and cross-border maritime enforcement in international waters much more difficult.

Key term:	Description
Maritime Chokepoint	A narrow, strategic waterway connecting two larger bodies of water, characterized by high concentrations of international

	commercial shipping and minimal maneuvering space. Primary global examples include the Bab al-Mandeb Strait, the Strait of Hormuz, the Suez Canal, the Strait of Malacca, and the Bosporus/Dardanelles Straits.
Asymmetric Warfare	Unconventional warfare conducted between opponents of vastly unequal military power or technological capabilities. In this context, it refers to non-state militias using low cost drones to neutralize multi-billion-dollar state naval vessels.
Anti-Access/Area Denial (A2/AD)	A defensive military strategy aimed at preventing an adversary from entering a specific geographic area (Anti-Access) or limiting their freedom of action within that area (Area Denial) via shore-based weaponry.
Dual-Use Goods	Commercial components, software, and technologies that are primarily designed for civilian industries (e.g., commercial agriculture drones, commercial GPS modules, recreational outboard boat motors) but can easily be weaponized or integrated into military-grade drone systems
Completely Knocked-Down (CKD) kits	Products or weapons shipped in parts and assembled at the destination. Non state militias heavily utilize CKD missile kits to slip through traditional interdiction operations undetected
Transit passage	Under part III of the united nations convention on the law of the sea (UNCLOS), the exercise of the freedom of navigation and overflight solely for the purpose of continuous and expeditious transit through an international strait
Freedom of Navigation Operations (FONOPs).	Operational naval maneuvers conducted by military forces to challenge what they

	consider excessive maritime claims by coastal states. These operations aim to preserve the rights, freedoms, and lawful uses of the sea and airspace guaranteed to all nations under international law. In the context of strategic chokepoints, FONOPs are frequently deployed to ensure transit corridors remain open, though their unilateral deployment can be a source of geopolitical tension between naval powers and coastal states.
Automatic Identification System (AIS)	An automated tracking system utilizing satellite and VHF radio transponders on vessels to broadcast unique identification, position, course, and speed data for maritime safety.
Ghost Fleet	A loose network of unflagged, falsely flagged, or poorly regulated commercial ships that deliberately deactivate maritime tracking systems to conduct illicit trade or transport sanctioned goods.
Ship-to-Ship (STS) Transfer	The operational transfer of cargo or fuel between seafaring vessels positioned alongside each other in international waters, frequently used by smugglers to break the legal chain of custody.
Plausible Deniability	A geopolitical strategy where an actor (typically a state sponsor) uses proxy networks or covert financial channels to hide their direct involvement in an aggressive action, leaving no explicit legal proof of accountability.
Transshipment Port	A high-volume international commercial hub where cargo is unloaded from one vessel and loaded onto another to alter destination paths, change container numbers, or falsify cargo manifests.
Hawaladar	An informal network broker who facilitates cross-border monetary value transfers based on honor, trust, and

	intra-network ledgers without utilizing formal digital wire transfers or conventional banks
Maritime Interdiction	The lawful military or regulatory operation of delaying, disrupting, or seizing a vessel and its cargo on high seas or in territorial waters to prevent the transit of illicit materials.
Inertial Measurement Unit (IMU)	An electronic module utilizing gyroscopes and accelerometers to calculate a vehicle's relative velocity, orientation, and gravitational forces, enabling autonomous navigation without satellite signals.
Militarization	The process by which a geographic area, commercial asset, or technology is systematically integrated into military strategic planning, equipped with defensive or offensive armaments, or transformed into a theater of kinetic warfare.
Prevention	Proactive legal, diplomatic, technical, or regulatory interventions designed to intercept, disrupt, or neutralize security vulnerabilities and illicit procurement funnels before they mature into active kinetic crises or open hostilities.
Proliferation	he rapid, unauthorized dissemination, transfer, or leakage of sensitive military hardware, software, manufacturing documentation, or dual-use technologies across sovereign borders to unauthorized state or non-state entities
Drone and Missile Technology	he convergence of uncrewed autonomous or remotely piloted aerial, surface, and sub-surface platforms (UAVs, USVs, UUVs) with advanced kinetic guidance packages, micro-propulsion subsystems, and precision-guided shore-to-sea ballistic/cruise weapon arrays
Non-State Actors	Any individual, syndicate, or entity operating independently of sovereign state control. In contemporary security frameworks, this expands beyond irregular insurgent militias and proxy networks to explicitly encompass Multinational Corporations (MNCs), private military contractors, and commercial defense/ aerospace conglomerates.

Key Challenges to International Security and Non-Proliferation

Tracking Vulnerabilities and the Dual-Use Procurement Loophole

The structural layout of modern globalized logistics provides an ideal environment for illicit procurement. Traditional non-proliferation networks are designed around finished ordnance manifests, tracking obvious military hardware like missile fuselages, solid-fuel rocket boosters, or specialized guidance computers. Non-state actors systematically exploit this baseline by utilizing a decentralized, fragmented sourcing mechanism known as the dual-use procurement loophole. Instead of purchasing completed military assemblies, procurement networks buy ordinary commercial components, such as civilian microchips, mass-market internal combustion engines, and industrial carbon-fiber tubing, under the guise of innocent civilian functions like agriculture or toy manufacturing.

Micro-Turbojets and Outboard Motors: These components are intentionally declared under harmless customs codes for commercial truck engine parts, agricultural lawnmowers, or water-well generators to avoid suspicion. Once smuggled into militia territory, they are re-engineered to provide extreme waterline speed for uncrewed surface vessels (USVs) or structural propulsion for land-to-sea cruise missiles.

Microchips and Transmitters: Procurement agents mix these vital electronics into massive shipments of consumer electronics or remote-controlled toy parts. Once acquired, they are uploaded with open-source software to build terminal autopilot systems, autonomous waypoint navigation modules, and live first-person view (FPV) video feeds for target tracking.

Carbon-Fiber and Fiberglass Tubing: These structural materials pass through international borders labeled as agricultural drainage tubes, water pipes, or wind turbine parts. Factions then utilize modular blueprints to bolt these segments together, transforming them into low-observable delta-wing drone hulls that drastically reduce radar cross-sections.

Because these individual components sit comfortably below the strict technical thresholds of export-control regimes like the Missile Technology Control Regime (MTCR), they easily evade traditional export audits. The committee faces the challenge of adapting legacy non-proliferation agreements so that they can better account for the cross-border flow of dual-use components without disrupting civilian commercial innovation and legitimate trade. Front companies purchase these items in bulk across neutral jurisdictions, moving them through high-volume transshipment ports where logistics agents alter cargo documentation and strip the original manufacturer records.

Consequently, standard customs enforcement agencies are left without a definitive mechanism to verify the lethal end-use intent of a commercial container shipment before it crosses into unmonitored coastal zones. Relying strictly on unilateral container checks is fundamentally insufficient against such adaptive smuggling funnels. Delegates must therefore focus their research on establishing expanded export tracking definitions, modernizing global customs protocols for commercial electronics, and building real-time data-sharing networks between global maritime registries and international intelligence operations. Resolutions should look past repetitive hardware descriptions to provide actionable legal and practical solutions that close these supply-chain tracking vulnerabilities, balancing stricter corporate auditing and downstream tracking for private tech multinational corporations (MNCs) with the preservation of civilian innovation and international trade liberties.

The Legal Vacuum of Sovereignty vs. Active Maritime Interdiction Protocols

The primary operational bottleneck when trying to counter chokepoint militarization is the basic tension between international maritime law and sovereign territorial integrity. Under Part III of the United Nations Convention on the Law of the Sea (UNCLOS), the right of Transit Passage guarantees foreign ships continuous navigation through strategic international straits, and coastal states may not suspend it. This right is not unlimited: under Article 39, transiting vessels must proceed without delay and refrain from any threat or use of force against the coastal state. This legal architecture protects the global economy from arbitrary blockades, but it simultaneously limits the operational capacity of international naval coalitions seeking to intercept smuggling pipelines.

Delegates should observe that a profound enforcement deadlock occurs the moment a suspected smuggling vessel enters a coastal state's Exclusive Economic Zone (EEZ). Under current international frameworks, a naval force cannot freely board a foreign-flagged civilian ship without obtaining explicit flag-state consent. If that consent is denied or ignored, international navies face an immediate legal gridlock, allowing the ship to safely enter sovereign territorial waters with its illicit cargo unless the vessel is stateless, falsely flagged, or explicitly subject to a United Nations Security Council (UNSC) inspection mandate.

While foreign navies enjoy the freedom of navigation on the high seas, their explicit authority to conduct active maritime interdictions inside an EEZ is highly restricted. Because UNCLOS assigns the primary responsibility for monitoring ships to their respective flag states, international navies lack a universal boarding treaty to intervene if a flag state lacks the technical infrastructure or political will to monitor its fleet. Existing legal tools fill only part of this gap. UNCLOS Article 110 allows a warship to board a vessel to verify its status only if it is suspected of being stateless or falsely claiming a flag. Similarly, the 2005 Protocol to the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) Convention and the voluntary Proliferation Security Initiative (PSI) allow boarding with flag-state authorization, but these frameworks focus almost exclusively on weapons of mass destruction (WMD) rather than the conventional dual-use parts fueling asymmetric chokepoint harassment.

This operational limitation creates a severe tactical paradox on land, where non-state actors frequently hide their mobile launchers and radar networks deep within civilian coastal infrastructure. A naval force can legally shoot down an incoming drone or missile over international waters to protect trade corridors. However, launching a retaliatory strike against a missile battery on land is generally prohibited by Article 2(4) of the UN Charter, which bars the use of force against another state's territory. Such a strike is lawful only if the Security Council authorizes it under Chapter VII, the host state consents, or it is justified as self-defense under Article 51. Sovereign states disagree sharply over whether self-defense applies to attacks launched by non-state groups from another country’s soil, a legal uncertainty that shields state sponsors and allows host nations to use their coastlines as safe zones for continuous maritime aggression.

Delegates must look for innovative pathways to bridge this jurisdictional divide by evaluating how existing maritime treaties and international frameworks can adapt to contemporary asymmetric realities. Resolutions should explore whether the international community requires expanded, consent-based multilateral boarding mechanisms in high-risk transit zones, or if states should instead focus on strengthening domestic border checkpoints and port security protocols. Delegates must ask themselves whether countering non-state maritime aggression demands the creation of new, complementary international legal instruments, or if the solution lies in building more robust, real-time intelligence-sharing networks that operate within the boundaries of existing state sovereignty

The Attribution Deficit and Asymmetric State Sponsorship

Modern asymmetric maritime warfare relies extensively on the attribution deficit to preserve regional stability and insulation for state sponsors. When a non-state militia fires an anti-ship cruise missile or coordinates a low-profile uncrewed surface vessel (USV) strike against a commercial vessel, the state sponsor providing the factory-built subsystems maintains plausible deniability. This diagnostic gap creates a severe digital forensic deficit, as the international community currently lacks a standardized, UN-backed technical protocol for digital flight data forensics and satellite telemetry tracking within international waters.

Uncrewed assets do not contain live operators, and the software steering them runs on open-source autopilot frameworks uploaded onto unlisted commercial microchips. When an uncrewed platform is intercepted or crashes, investigator teams face several distinct technical challenges that complicate accountability. Procurement networks systematically erase physical serial markings, factory country stamps, and regulatory identifiers from guidance microchips to disrupt origin tracing, while integrated Inertial Measurement Units (IMUs) use local dead-reckoning algorithms to navigate completely without leaving an active radio frequency signature to track back to a specific base. Furthermore, militias utilize commercial satellite internet terminals covered in radar-absorbent resin, successfully routing live steering signals through global proxy servers and shifting legal footprints across neutral borders.

Concealment of Guidance Subsystems: Procurement networks systematically erase or destroy physical serial markings, factory country stamps, and regulatory identifiers from guidance microchips to disrupt origin tracing.

Autonomous Localized Navigation: Integrated Inertial Measurement Units (IMUs) use local dead-reckoning algorithms that run directly on the drone, meaning the platform can navigate completely when satellite links are jammed, leaving no active radio frequency signature to track back to a specific base.

Masked Communication Architecture: Militias utilize commercial satellite internet terminals covered in radar-absorbent resin, successfully routing live steering signals through global proxy servers and shifting legal footprints across neutral borders.

The committee must confront the diplomatic paralysis caused by this forensic vacuum. Without ironclad forensic proof directly connecting a sovereign state's military infrastructure to a specific chokepoint attack, the United Nations Security Council (UNSC) frequently encounters legislative deadlocks. Member states are forced to rely on unilateral intelligence findings, which often breeds deep political mistrust and prevents the international consensus needed to enforce targeted arms embargoes. Consequently, state sponsors can continuously outsource maritime aggression to regional proxies without facing immediate economic, legal, or geopolitical consequences.

Resolutions should aim to bridge this investigative gap by exploring how technical cooperation can be strengthened with international bodies like the International Maritime Organization (IMO) and the United Nations Office for Disarmament Affairs (UNODA). Delegates must ask themselves whether the international community should establish uniform legal criteria for tracking digital flight data and verifying weapon component forensics, or if states should instead focus on developing non-physical tracing mechanisms embedded at the manufacturing level. The challenge for the committee is to determine if countering the attribution deficit requires the integration of next-generation chemical taggants within raw industrial components, or if the solution lies in creating new multilateral intelligence-sharing frameworks that protect national sovereignty while permanently securing the global supply chain.

Case Studies

1) The Bab al-Mandeb Strait and the Red Sea Crisis

The Bab al-Mandeb Strait, a narrow 29-kilometer-wide maritime corridor separating the Arabian Peninsula from the Horn of Africa, serves as a vital economic artery connecting the Indian Ocean to the Mediterranean Sea via the Suez Canal. Historically, maintaining security within this bottleneck relied on state-centric conventional naval deterrence, managed by international task forces deployed to suppress low-tech piracy. However, the systemic collapse of central state authority in adjacent coastal territories allowed a highly organized non-state militia to establish a robust anti-access/area-denial (A2/AD) coastal footprint. This transformation has made the Red Sea a major theatre of asymmetric maritime conflict.

Instead of deploying capital-intensive naval warships, the militia utilizes decentralized proxy supply chains to acquire Completely Knocked-Down (CKD) kits, assembling long-range loitering munitions, anti-ship cruise missiles (ASCMs), and explosive-laden uncrewed surface vessels (USVs) deep within civilian infrastructure. The tactical execution of these asymmetric blockades has exposed massive vulnerabilities in global commerce. Commercial container ships and energy tankers passing through the strait are routinely subjected to coordinated loitering munition swarms and land-based ballistic strikes. This persistent threat forced international shipping conglomerates to alter their transit routes entirely, diverting hundreds of vessels away from the Suez Canal and around the Cape of Good Hope. This re-routing added thousands of extra nautical miles to global shipping voyages, delayed manufacturing supply lines by weeks, and caused global maritime insurance premiums to surge exponentially.

This case study serves as a critical template for the committee because it perfectly illustrates the limits of purely defensive naval operations over water. In response to the crisis, multilateral naval coalitions initiated protective interception maneuvers in international shipping lanes, successfully destroying inbound drones and missiles mid-air. However, this defensive strategy operates at a severe economic and tactical disadvantage, as multi-million-dollar naval air defense missiles are continuously expended to neutralize low-cost consumer-grade drones. Furthermore, while international forces can protect merchant hulls over the water, the core threat infrastructure—including mobile transporter-erector-launchers (TELs) and hidden assembly facilities—remains safely insulated deep within land borders.

Delegates should analyze how any attempt to launch retaliatory kinetic strikes against these land-based targets risks violating Article 2(4) of the UN Charter, threatening to expand localized maritime skirmishes into a broader regional war. Resolutions must consequently address how DISEC can design frameworks to disrupt the supply chains feeding such a crisis at its structural source before asymmetric littoral blockades cause irreversible economic disruption.

2) The Strait of Hormuz

The Strait of Hormuz, the gateway from the Persian Gulf to the Gulf of Oman and the Arabian Sea, channels approximately 20% of the global petroleum supply. Since 2026, it has become the clearest example of a chokepoint closed by force. Iran has sought to control the Strait through threatened and actual attacks on commercial shipping since the US-Israeli strikes on Iran began on 28 February 2026. On 2 March, the Islamic Revolutionary Guard Corps (IRGC) declared the Strait closed to “unfriendly nations,” allowing only Iran-approved vessels to pass. The United States blockaded Iranian ports from 13 April to 29 May. A ceasefire in April and a June memorandum were followed by renewed fighting in July. In June, US Central Command (CENTCOM) reported Iranian one-way attack drones aimed at commercial ships, and the US military has since announced it cleared mines Iran laid in the shipping lanes. The attacks continue, and the commercial sector bears the cost, with Windward estimating that Iran attacked roughly two ships for every 100 that crossed the Strait in the third quarter of 2026, while freight costs represent 25–30 percent of Gulf crude's cost compared to just 1–3 percent before the war. The crisis has killed dozens of seafarers and port workers. Oil volumes continue attempting to move through the chokepoint via naval escorts, even as attacks on tankers accelerate.

Hormuz differs from the Red Sea in one decisive way: the principal actor is a state, so attribution is not the main difficulty. Iran openly asserts control of the passage. The non-state dimension lies elsewhere. The Houthis resumed attacks on shipping in the Red Sea and Gulf of Aden in July, adding pressure to supply chains already strained by Iran’s efforts to close Hormuz. Reporting describes the Houthi campaign against energy exports as consistent with Iran’s strategy of constraining global energy supplies to pressure the United States. Since 2 October, United Kingdom Maritime Trade Operations (UKMTO) has reported at least one attack a day in the Strait of Hormuz or the Gulf of Aden. A single state’s strategy is thus being carried out at two chokepoints at once, in one case directly and in the other through a non-state armed group. Shipping companies, insurers, and seafarers are non-state actors too, and they bear the consequences of both. This case belongs in this guide because the weapons are of the same class as those used by non-state armed groups, namely low-cost one-way attack drones and sea mines, meaning export controls, tracking protocols, and intelligence-sharing mechanisms could apply to both. Legal status adds to the difficulty: Iran signed but never ratified UNCLOS and disputes that the transit passage regime binds it.

Delegates should carefully analyze how the intersection of state strategy and asymmetric weapon systems reshapes the committee's traditional mandate. Resolutions should evaluate whether tracking frameworks designed to disrupt supply chains to armed groups can be conceptually expanded to address state actors utilizing the same classes of commercialized technology, or if these two operational dimensions must remain structurally distinct. Furthermore, the committee must assess how a recommendatory body can meaningfully intervene when core stakeholders within international security bodies remain deeply divided over strategic responses to active chokepoint blockades. Finally, delegates must look into the necessary protections and standardized reporting frameworks that should apply to private commercial operators to support crew welfare, stabilize maritime insurance architectures, and streamline incident communications with global regulatory bodies.

3) The Strait of Malacca

The Strait of Malacca, stretching between the Indonesian island of Sumatra, peninsular Malaysia, and Singapore, is the primary economic artery linking the Indian Ocean to the South China Sea and East Asian manufacturing economies. Historically, the strait has been categorized as a low-intensity maritime security zone, defined by localized criminal piracy syndicates executing low-tech financial extortion against merchant vessels. However, the rapid global democratization of precision flight technologies creates a severe preventative security threat for Southeast Asian waterways, as the potential acquisition of commercial off-the-shelf (COTS) drone hardware by organized transnational crime rings or localized militant groups could rapidly outpace current law enforcement capabilities.

The modern risk architecture in the Malacca Strait centers on the potential migration of asymmetric warfare tactics from active conflict zones to commercial channels. If pirate networks transition from high-risk physical boarding operations to remote tactical harassment, modifying consumer-grade quadcopters or heavy-lift logistics drones to carry gravity-dropped submunitions, they could project lethal force across the strait's narrowest channels, which constrict to just 2.8 kilometers near Singapore. Because these automated systems can be operated remotely from land with high operational deniability, they present a profound threat to an artery that carries over 35% of global seaborne oil.

Delegates should carefully analyze how this region highlights the deep operational reliance on the United Nations Convention on the Law of the Sea (UNCLOS). Because the Strait of Malacca is governed by the strict doctrine of Transit Passage, the littoral states bear the exclusive legal responsibility for domestic maritime law enforcement. Traditional naval patrols cannot easily secure dense coastal mangrove forests against mobile land-based operations, and because drone components are classified under everyday civilian electronics codes on customs manifests, regional port authorities lack the data-sharing infrastructure to intercept components before they reach coastal zones.

Resolutions must consequently evaluate how preventative capacity-building models can reinforce regional intelligence-sharing networks, such as building upon existing state frameworks like the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP), to track dual-use hardware flow before criminal actors exploit these technical legal gaps.

4) The Suez Canal

The Suez Canal, an artificial waterway slicing through Egyptian territory, serves as the ultimate maritime link between European markets and Asian production hubs. Unlike the open water lanes of natural straits, the canal is entirely enclosed within the national borders of a single sovereign state, granting Egypt exclusive administrative jurisdiction and sole responsibility for transit security. This centralized layout historically shielded the waterway from the jurisdictional ambiguities that plague natural chokepoints. However, the geographic containment of the canal has exposed severe defensive limitations in the face of modern asymmetric weapons.

The operational vulnerability of artificial channels became starkly evident during the July 2026 Damietta port drone strike, where an unclaimed aerial attack ignited a major fire on a U.S.-owned liquefied natural gas (LNG) storage tanker right at the Mediterranean entrance to the Suez corridor. This incident underscored that even when a sovereign state maintains tight domestic military control over its banks, asymmetric weapon systems can be launched outside its territorial boundaries to strike ships inside its terminal ports. Because the canal serves as the prime detour route for oil attempting to bypass active conflict zones like the Strait of Hormuz, localized drone strikes in Egyptian ports create an immediate risk of multiplying war-risk insurance premiums and throttling European energy security.

Delegates should observe how artificial waterways alter the legal debate surrounding maritime safety. Because the canal operates under sovereign state regulations rather than the universal Transit Passage doctrine of natural straits, external naval task forces cannot conduct autonomous protective operations within its waters. Resolutions should explore how the international community can support sovereign host nations with advanced technical defense hardware, cyber-security data-sharing pipelines, and port-monitoring protocols without infringing upon national border control.

National perspectives

1) United States of America

As the world's primary naval power and the chief architect of the contemporary global maritime security architecture, the United States views the militarization of chokepoints by non-state actors as an existential threat to its national security and international trade. The US strategic doctrine emphasizes absolute freedom of navigation and the immediate protection of commercial transit corridors, particularly in the Bab al-Mandeb and the Strait of Hormuz.

The US policy priority centers on utilizing multilateral naval coalitions, such as Combined Task Force 151, to conduct active maritime interdiction operations. To advance these goals, the United States strongly advocates for reforming UN Security Council Resolution 1540 to expand its scope beyond traditional weapons of mass destruction, thereby capturing the flow of conventional dual-use drone parts to non-state actors. Furthermore, the US supports implementing a binding Universal Component Marking System to force global tech manufacturers to laser-etch trackable regional codes onto commercial microchips. As a non-party to UNCLOS, the United States favors a stronger consent-based boarding framework, built through flag-state agreements, the Proliferation Security Initiative, and Security Council-authorized inspections, which would reach unflagged or falsely flagged Ghost ships without amending UNCLOS. The US explicitly rejects arguments that land-based counter-battery strikes violate Article 2(4) of the UN Charter, asserting its inherent right to self-defense under Article 51 when protecting its military assets and commercial vessels from persistent littoral bombardment.

2) Islamic Republic of Iran

The Islamic Republic of Iran’s perspective is anchored in the preservation of regional hegemony and strict opposition to Western military deployment along its coastal borders. Iran asserts that the primary cause of instability in strategic waterways, specifically the Strait of Hormuz, is the over-saturation of unilateral foreign naval forces, which it views as a direct violation of the sovereignty of littoral states.

Iran’s diplomatic strategy focuses on protecting its strategic depth and resisting international export restrictions. Iran, which signed but has never ratified UNCLOS, strongly opposes any modification to the Convention, any new arrangement, or any expanded reading of existing rules that would grant foreign navies expanded interdiction or boarding rights within Exclusive Economic Zones, labeling such proposals as Western maritime imperialism. Additionally, Iran resists the implementation of tracking protocols like the Universal Component Marking System, arguing that broad component markings place unfair economic burdens on developing economies and restrict access to commercial civilian hardware. Iran maintains that regional security must be managed exclusively by the coastal states themselves through localized treaties. It utilizes its geographic position along the Strait of Hormuz to project defensive anti-access/area-denial capabilities, arguing that its domestic military development is purely defensive and designed to counter foreign aggression.

3) Kingdom of Saudi Arabia

Positioned between the Red Sea and the Persian Gulf, the Kingdom of Saudi Arabia is uniquely vulnerable to the militarization of both the Bab al-Mandeb and the Strait of Hormuz. Having led a regional coalition against insurgent forces along its southern border, Saudi Arabia views the proliferation of asymmetric drone and missile technology to non-state actors as an immediate challenge to its territorial integrity and its Vision 2030 economic diversification plans.

Saudi policy balances aggressive counter-proliferation measures with a desire to maintain regional stability. Saudi Arabia firmly supports the enforcement of strict, targeted United Nations (UN) arms embargoes, modeled on traditional international sanctions regimes, to cut off smuggling funnels feeding non-state proxies. The Kingdom also champions the disruption of the financial architectures of proliferation, calling for international banking task forces to track and dismantle the informal Hawala networks and anonymized cryptocurrency channels used by procurement agents. To support these enforcement actions, Saudi Arabia seeks increased technical capacity-building from the United Nations Office for Disarmament Affairs (UNODA) to modernize its border security and port inspection infrastructure. Saudi Arabia emphasizes that maritime security frameworks cannot operate effectively without directly neutralizing the land-based assembly plants and state-proxy financial networks funding asymmetric forces.

4) Republic of Singapore

\As a classic littoral state situated at the nexus of the Strait of Malacca and the Singapore Strait, Singapore's survival depends entirely on unhindered global maritime trade. Singapore views any disruption to transit corridors as an immediate threat to its economic lifeblood, but its diplomatic position is defined by strict adherence to international law and multilateralism.

Singapore's strategy prioritizes localized coordination over unilateral foreign military intervention. Singapore's key policy alignments include maintaining the absolute integrity of the United Nations Convention on the Law of the Sea (UNCLOS) Part III, ensuring that the rules governing Transit Passage remain an international right rather than a negotiable privilege and that littoral states retain final domestic jurisdiction over their territorial waters. The nation actively promotes regional information-sharing models, such as the Information Fusion Centre (IFC) situated at Changi Command and Control Centre, which coordinates an integrated team of International Liaison Officers to share real-time maritime data and track non-compliant vessels without surrendering command authority to global powers. Furthermore, Singapore supports non-disruptive export reforms that tighten customs verification protocols for dual-use electronics at major transshipment hubs without slowing down global supply chains. Singapore argues that the most effective way to counter asymmetric maritime threats is to build up the maritime law enforcement capacity of vulnerable coastal states rather than relying on external naval coalitions.

5) Arab Republic of Egypt

Egypt is one of the primary economic casualties of maritime instability at global chokepoints. Because the Bab al-Mandeb Strait serves as the southern gateway to the Suez Canal, the Red Sea crisis sharply reduced canal traffic and deprived Egypt of billions of dollars in vital sovereign transit revenue. The canal earned a record $9.4 billion in fiscal year 2022/23. Revenue rose 23% to $4.67 billion in fiscal year 2025/26 as more vessels returned, but that is still only about half the peak. Second-quarter 2026 revenue reached $1.26 billion, up 13% on the previous quarter, the highest quarterly level since the first quarter of 2024.

Egypt's position balances its urgent economic need for maritime stability with its commitment to traditional non-intervention and state sovereignty. The state advocates for diplomatic solutions within the framework of the United Nations to de-escalate regional tensions, arguing that purely military naval interventions fail to address the root political catalysts of disputes. Egypt also supports strengthening multilateral tracking tools in cooperation with the International Maritime Organization (IMO) to identify and penalize private shipping registries that allow non-compliant fleet vessels to operate unmonitored. To alleviate the financial strains of the crisis, Egypt pushes for securing international financial support or regulatory subsidies for developing trading nations whose economies are disproportionately affected by rising maritime insurance premiums and trade diversions. However, Egypt strongly resists any counter-proliferation protocols that would grant foreign navies the unilateral right to conduct kinetic operations within the sovereign waters or territorial coastlines of developing states.

Questions Any Resolution Must Answer (QARMA)

Questions Any Resolution Must Answer (QARMA) are the core questions that delegates must resolve when writing their committee resolutions. These questions act as a final checklist for the committee, guiding your research and ensuring that the final documents provide realistic, practical solutions to every dimension of the crisis rather than just repeating general statements about maritime safety.

1) How can the international community update export control agreements, such as the Missile Technology Control Regime (MTCR), to track low-cost civilian drone parts without harming global technology industries?

2) How can member states develop standardized, consent-based regional interdiction frameworks and bilateral tracking agreements to counter the smuggling of Completely Knocked-Down (CKD) kits without structurally amending the established provisions of UNCLOS?

3) How can DISEC facilitate diplomatic conflict-prevention protocols and intelligence-sharing networks to isolate and neutralize land-based threat infrastructures before kinetic escalation occurs?

4) What institutional frameworks should be co-developed with the International Maritime Organization (IMO) and UNODA to create a unified database for tracking digital flight telemetry, open-source autopilot logs, and hardware component forensics to counter state-sponsored proxy deniability?

5) What concrete measures should member states adopt to track, freeze, and dismantle the illicit Financial Architectures of Proliferation supporting non-state militias, specifically regarding anonymized cryptocurrency transactions and the informal Hawala trust broker system?

6) What guidelines and transparency frameworks can DISEC recommend to encourage flag states to track, register, and report the deployment of autonomous uncrewed surface vessels (USVs) and semi-submersibles in strategic straits?

7) In what ways can DISEC facilitate technical capacity-building and real-time data-sharing between global container shipping registries and vulnerable littoral states to detect falsified customs manifests and container swaps at transshipment ports?

8) What multilateral mechanisms or UN-backed safety nets can be established to safeguard global supply chains and protect developing trading nations from soaring maritime insurance premiums and systemic trade extortion during active chokepoint crises?

Reference

International Court of Justice. Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment, 1986.

International Maritime Organization. https://www.imo.org/en/OurWork/Safety/Pages/Default.aspx *Guidelines on Automatic Identification System (AIS) Deactivation and Vessel Tracking Metrics*, 2024.

Missile Technology Control Regime. https://www.mtcr.info/en/mtcr-guidelines Equipment, Software, and Technology Annex, 1987.

United Nations. https://www.un.org/en/about-us/un-charter/chapter-7 Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, 1945.

United Nations. https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf Part III: Straits Used for International Navigation, 10 December 1982.

United Nations General Assembly. First Committee (DISEC) Main Page. Mandate, Structural Progression, and Resolutions, United Nations Office for Disarmament Affairs (UNODA), 2023.

United Nations Office for Disarmament Affairs. https://www.un.org/disarmament/convarms/register/ Transparency in Procurement and Completely Knocked-Down (CKD) Tracking Issues, 2025.

United Nations Security Council. https://digitallibrary.un.org/record/520326?v=pdf Non-Proliferation of Weapons of Mass Destruction and Non-State Actor Mandates, 28 April 2004.

United Nations Security Council. https://digitallibrary.un.org/record/791250/ . Sanctions Reinforcement, Non-State Targeted Arms Embargoes, and Interdiction Frameworks in Yemen, 14 April 2015.

United Nations Security Council Sanctions Committees. https://www.un.org/securitycouncil/sanctions/information Prohibited Item Tracking and Asset Freeze Master Manifests for Somalia, Libya, and Yemen, 2022