

55MUNVII

UNSC



STUDY GUIDE

TABLE OF CONTENTS

1. Crisis Documentation
2. About the committee's Mandate
3. War On Terror
4. Weaponization of Undersea Infrastructure
5. Quantum Espionage

Crisis Documentation

1. Directives :

Directives instead of resolutions to make recommendations and take action will be used. Delegates will write multiple smaller, handwritten directives to address specific issues as they arise with each update. While directives are ideally structured and well formatted with operative clauses, given the handwritten and non-traditional format of these documents, the dais will be more lenient in downgrading and accepting such documentation.

a. Private Directives:

A Private Directive (Crisis Note) is used to advance a personal agenda. These actions can remain discreet or become public. To be effective, notes must be creative, realistic, and concisely written (well- detailed) within the limits of an allotment's powers. Overly long, poorly planned (with loopholes and/or vagueness) , or unrealistic actions will be rejected immediately. Whether an action succeeds depends entirely on the directive's quality and upon the discretion of the dais. Joint Private Directives will also be accepted which combine the powers of two or more delegates to execute complicated actions that an individual's powers cannot achieve alone. These bypass a committee vote and are approved or denied solely at the discretion of the dais.

1 b. Short-term Directives :

Respond to, solve, or exploit the loopholes in the immediate crisis update at hand.

2 c. Long-term Directives :

Lay the foundation for a strategic plan that comes into motion later in the course of the committee.

Common types of directives accepted by the dais include (but are not limited to):

a. Recruitment directives :

Used within the committee to secure political backing or recruit personnel for the committee or the delegate's personal forces.

b. Military directives:

Strategic military actions executed through powers in the committee. These must include precise details regarding the strategy, troop count, and target area.

c. External communications:

Shared as Public Service Announcements, or Invitations/Requests to contact any individual or group outside the committee.

d. Intelligence directives:

Actions used to collect data, spread information, or execute disruptions including interceptions of other directives.

e. Assassinations:

Operations requiring exceptional planning and strategy. Repeating poorly planned attempts will result in penalties and downmarking.

2. Public Directives :

Public Directives are official actions taken collectively by the committee as a whole. In terms of procedure and formatting, they operate much like traditional Working Papers. Unlike private or joint private directives, which remain confidential, Public Directives are entirely transparent and must be formally presented to the floor, debated, and voted on by the room to pass. To excel in this area, delegates must show a strong sense of initiative and propose creative solutions to the issues at hand. Success depends heavily on your ability to foster collaboration, build consensus, and reconcile opposing viewpoints to get the directive passed by the majority.

3. Press Releases:

A press release is a public document issued by your portfolio to the media and the general public. While crisis notes are secret, press releases are completely open and transparent.

Rules of engagement for a press release:

- I. Must be submitted directly to the crisis desk for approval before it impacts the simulation.
- II. Used to sway public opinion, issue official denials, or broadcast a policy shift. It cannot execute secret covert actions.
- III. Must be written in a formal, authoritative, and in-character journalistic voice.
- IV. The public will react to your statements. Misinformation, poorly timed announcements, or radical declarations can trigger public unrest, market crashes, or diplomatic fallout.

To pass, your release must meet the following criteria:

- I. Authority: You must have the institutional power to speak on the topic.
- II. Factuality: You can only announce actions, resources, or policies that your character actually possesses or has already executed.
- III. Relevance: The content must directly address the current, active crisis timeline.
- IV. Professionalism: The tone must remain strictly formal, diplomatic, and in-character.
- V. Intent: The release must have a clear, actionable goal for how it is trying to shift public perception.

Sample Private Directive:

Operation Red Decree: part 1

To my confidant,

All these messages to you from now will be sown into the robe seams of the messengers delivering them.

After implementing them, burn the letters.

Send a letter to the Quaestor in charge of public revenue. Tell him that in exchange for 300,000 silver denarii and his silence about these dealings, with immediate effect I can make a Holy Augur bless his fortunes and vouch his success to the senate. I can also use my political connections with Mark Antony to progress his political career in exchange for continued support. I expect you to be discreet.

About the Committee's Mandate

Formed in 1945 under the Charter of the United Nations, the United Nations Security Council (UNSC) is the principal UN organ entrusted with the maintenance of international peace and security. Under Article 24(1) of the UN Charter, Member States confer on the Council “primary responsibility for the maintenance of international peace and security” and agree that, in carrying out those duties, it acts on their behalf. The Council differs from most other UN organs because it can adopt decisions that Member States are legally obligated to carry out under Article 25. Its powers are principally contained in Chapters VI, VII, VIII and XII of the Charter, and include peaceful dispute settlement, sanctions, establishment of peacekeeping operations, authorization of force and measures concerning threats to international peace and security.

The Council consists of 15 members: five permanent members and ten non permanent members elected by the General Assembly for two-year terms under Article 23. Under Article 27, substantive decisions require at least nine affirmative votes, including the concurring votes of the permanent members. In practice, a permanent member's abstention does not prevent adoption if the nine-vote threshold is met; a negative vote by a permanent member constitutes a veto.

Unlike other UN entities, the Council's decisions are legally binding on all recognized member states, enabling it to enforce them through diplomatic, economic, or military measures. Its main role is to uphold international peace and security. To fulfill this responsibility, the Council can approve peacekeeping

operations, impose sanctions, cut off diplomatic or economic ties, and, when required, authorize the use of armed force. It may also display military capability, such as through blockades or patrols, as part of its enforcement powers.

The UNSC's objectives correspond to the four central purposes of the United Nations:

- ★ Maintain international peace and security
- ★ Foster friendly relations between nations
- ★ Promote cooperation in addressing global challenges ★ Encourage respect for human rights

The Council has fifteen members. Five are permanent members with veto power, granted in recognition of their role in founding the UN:

- ★ The People's Republic of China
- ★ The French Republic
- ★ The Russian Federation
- ★ The United Kingdom
- ★ The United States of America

The other ten seats are filled by non permanent members, elected by the General Assembly for two year terms through a two thirds majority vote. These members are not eligible for immediate re election. The Council's presidency rotates every month among all members in alphabetical order. Each member casts one vote on draft resolutions. For a resolution to pass, it must receive at least nine votes in favor and no veto from any permanent member. Permanent members may abstain, and an abstention does not block adoption if the nine vote requirement is met. All resolutions passed by the Council are legally binding under Article 25 of the UN Charter.

This is an open agenda committee.

Sub Topic #1: War On Terror 2001

1) Origins:

During the 1990s, al Qaeda, founded by Osama bin Laden, developed into a transnational terrorist organisation with bases in Afghanistan and networks across several countries. Its attacks included the 1998 United States embassy bombings in Kenya and Tanzania, which killed more than 200 people, and the October 2000 bombing of the USS Cole in Yemen, which killed 17 US personnel. The Taliban, which controlled most of Afghanistan by 1996, provided al Qaeda with sanctuary. On 11 September 2001, al Qaeda carried out attacks in the United States, killing approximately 3,000 people. The attacks prompted the US led campaign commonly called the War on Terror, which was a combination of military operations, intelligence, counterterrorism legislation, financial restrictions and security measures.

2) Resolution 1368 (2001):

- a. On 12 September 2001, the Security Council adopted Resolution 1368, which condemned the 9/11 attacks and recognised the inherent right of individual and collective self defence in accordance with the UN Charter. It called on States to cooperate in bringing the perpetrators, organisers and sponsors to justice and to prevent further terrorist attacks. The resolution was the basis for international, legal, and political context for the subsequent counterterrorism response, but it did not authorise a specific military operation or identify every State against which force could be used.

3) Operation Enduring Freedom and the Invasion of Afghanistan in 2001:

- a. On 7 October 2001, the United States and the United Kingdom began military operations in Afghanistan under Operation Enduring Freedom, targeting al Qaeda and Taliban military positions after the Taliban failed to meet US demands concerning al Qaeda and Osama bin Laden. The campaign combined air strikes with Afghan anti Taliban forces, including the Northern Alliance. Kabul fell to anti Taliban forces in November 2001, followed by the collapse of the Taliban's remaining strongholds. The operation had aimed to

dismantle al Qaeda's Afghan infrastructure and remove the Taliban government that had provided it a sanctuary. Its legal basis was asserted by the participating States through the right of self defence under Article 51 of the UN Charter; the Security Council did not adopt a resolution expressly authorising the invasion. Resolution 1368 recognised the right of self defence, while Resolution 1373 subsequently established binding counterterrorism obligations for all UN Member States.

4) Battle of Tora Bora in December 2001:

- a. The Battle of Tora Bora was fought in eastern Afghanistan in December 2001, and was an operation by US forces and Afghan allied forces against al Qaeda fighters in mountainous terrain near the Pakistan border. US officials believed Osama bin Laden was present in the area, but he escaped. The failure to capture him became an early setback in the campaign against al Qaeda's leadership. The battle was also a demonstration of the operational difficulties of pursuing transnational armed groups across remote terrain and near international borders. Bin Laden remained at large until he was killed by US forces in Abbottabad, Pakistan, in May 2011.

5) Security Council Resolution 1373 of 2001, and the Counter Terrorism Committee:

- a. On 28 September 2001, the Security Council unanimously adopted Resolution 1373 under Chapter VII of the UN Charter, which created binding obligations for all Member States. States were required to criminalise terrorist financing, freeze funds and financial assets associated with terrorism, prevent the provision of support to terrorist groups, deny safe haven to those involved in terrorist acts and work towards strengthening international cooperation in investigation, extradition and prosecution. The resolution also established the Counter Terrorism Committee (CTC) to monitor implementation. Unlike earlier resolutions addressing particular situations, Resolution 1373 was a broader framework applicable to all UN Member States without establishing a single universal definition of terrorism. In 2004, Resolution 1535 established the Counter Terrorism Committee

Executive Directorate (CTED) to support the CTC through assessments and technical assistance.

6) Resolution 1378 of 2001 and the Transition in Afghanistan:

- a. On 14 November 2001, the Security Council adopted Resolution 1378, which supported international efforts to establish a new Afghan administration and emphasized that the United Nations should play a role in assisting the Afghan people in establishing a representative government. It stated that an inclusive political process is needed, and rejected the restoration of the Taliban's control. The resolution formed part of the diplomatic response to the collapse of Taliban rule. In December 2001, the Bonn Agreement established an interim political framework for Afghanistan, and Resolution 1386 authorised the International Security Assistance Force (ISAF) to assist in maintaining security in and around Kabul. ISAF later expanded its operations across Afghanistan.

7) Guantánamo Bay:

- a. In January 2002, the United States began to transfer detainees captured in connection with the War on Terror to the detention facility at Guantánamo Bay, Cuba. The US administration was arguing that certain detainees could be held as enemy combatants outside the ordinary criminal justice system. The facility then became associated with indefinite detention, disputed interrogation practices, restrictions on access to legal remedies as well as the use of military commissions. The legal controversy concerned the applicability of the Geneva Conventions, the authority of the executive branch and detainees' access to judicial review. The US Supreme Court ruled in *Hamdan v. Rumsfeld* (2006) that the military commissions that were established under the administration's framework were a violation of the Uniform Code of Military Justice and law of war requirements.

8) CIA Black Sites:

- A. Following 9/11, the Central Intelligence Agency operated a secret detention and interrogation programme involving facilities outside US territory, commonly described as black sites.

Detainees were held at undisclosed locations, including facilities associated with countries in Europe and Asia, while some suspects were transferred between jurisdictions through extraordinary rendition. Investigations by the Council of Europe and other bodies documented secret detention facilities and the involvement of several States. Poland and Lithuania were among the European countries examined in investigations concerning CIA detention; Thailand was also associated with the programme.

9) ***1999 Convention, FATF, Sanctions and Hawala:***

- A. The International Convention for the Suppression of the Financing of Terrorism was adopted by the General Assembly on 9 December 1999 and entered into force on 10 April 2002. It requires States Parties to criminalise the financing of terrorist acts, establish jurisdiction, cooperate in investigations and facilitate the identification, freezing and seizure of funds used to finance terrorism. Resolution 1373 also requires States to suppress terrorist financing and freeze assets. The Financial Action Task Force (FATF) developed standards to combat money laundering and terrorist financing, including criminalisation, financial monitoring and financial sanctions. Hawala is an informal value transfer system that can serve remittance needs but may be exploited for illicit finance when transactions evade effective oversight.

10) ***Incitement to Terrorism:***

- A. On 14 September 2005, the Security Council adopted Resolution 1624, which addressed the incitement of terrorist acts. It called on States to prohibit by law the incitement to commit terrorist acts, prevent such conduct and deny safe haven to individuals against whom credible and relevant information indicated involvement in such incitement. It also emphasised that counterterrorism measures must comply with international human rights law, refugee law and international humanitarian law. The resolution expanded the international counterterrorism framework beyond the financing and operational support of terrorist groups to include the prevention of terrorist incitement, while leaving implementation to national legal systems consistent with international obligations.

11) Hamdan v. Rumsfeld in 2006:

A. On 29 June 2006, the US Supreme Court ruled 5–3 in *Hamdan v. Rumsfeld* that the military commission established to try Salim Ahmed Hamdan under the administration's existing framework lacked legal authority to proceed because its structure and procedures violated the Uniform Code of Military Justice and applicable law of war requirements, including Common Article 3 of the Geneva Conventions. The judgment did not declare every form of military commission unlawful; it held that the commissions in question could not operate under the framework then established. Congress subsequently enacted the Military Commissions Act of 2006, creating a statutory basis for revised commissions. The case became a major precedent concerning executive authority, military detention and the application of legal protections during the War on Terror.

12) Suicide Bombings:

B. The War on Terror coincided with major terrorist attacks in Europe. On 11 March 2004, coordinated bombings of commuter trains in Madrid killed 191 people and injured approximately 2,000; the attacks were attributed to an Islamist extremist cell rather than directly to al Qaeda's central leadership. On 7 July 2005, four suicide bombers carried out attacks on London's public transport system, killing 52 victims in addition to the bombers and injuring hundreds. These attacks demonstrated the capacity of extremist networks and individuals operating within European societies to conduct mass casualty attacks. The European response included strengthened intelligence sharing, border cooperation, domestic counterterrorism legislation and increased attention to recruitment, radicalisation and terrorist financing. The incidents also highlighted the distinction between organisations directly commanded by al Qaeda and individuals or groups influenced by its ideology.

12) Doha Agreement of 2020:

A. On 29 February 2020, the United States and the Taliban signed the Agreement for Bringing Peace to Afghanistan in Doha, Qatar. The agreement provided for the

withdrawal of US and allied forces within 14 months, subject to its terms, alongside Taliban commitments concerning the prevention of terrorist groups using Afghan territory to threaten the United States and its allies. It also envisaged the commencement of intra Afghan negotiations and discussions concerning a permanent ceasefire. The Afghan government was not a signatory to the US–Taliban agreement, although a separate US–Afghan joint declaration was issued. US forces completed their withdrawal in August 2021 as the Taliban regained control of Afghanistan. The agreement marked the end of the US military presence in Afghanistan but did not itself establish a comprehensive peace settlement between the Taliban and all Afghan political actors.

Key terms and Definitions

1) Pre-emptive War:

A military conflict which is initiated because a state believes that an enemy attack is imminent and that striking first is necessary to prevent or reduce the damage of that attack.

In the context of the War on Terror, the term has great importance because US policymakers increasingly discussed striking terrorist organizations and hostile states present within Muslim Countries before they could carry out attacks against the United States or its allies.

Following the September 11 attacks, the United States invoked Article 51 to justify military action against al Qaeda and the Taliban regime in Afghanistan, the validity of the invocation of Article 51 is though widely questioned by the allies and the affected countries.

2) Axis of Evil

The Axis of Evil was a term introduced by US President George W. Bush in his 2002 State of the Union address.

However, the three states had different political objectives and relationships with militant groups; and grouping them together was considered highly controversial,

which further contributed to the exacerbation of violence surrounding the 2003 Iraq War, whose central claims about active weapons of mass destruction stockpiles were subsequently discredited.

3) F3EAD:

F3EAD stands for Find, Fix, Finish, Exploit, Analyze, and Disseminate which is an American military strategy used to identify targets, carry out operations, collect information, and share intelligence. During the War on Terror, especially in Iraq and Afghanistan, it helped military forces use information from one operation to plan future actions and improve their understanding of terrorist networks. However, it also raised concerns about incorrect intelligence and civilian casualties

4) Counter IED:

Refers to an intelligence led and coordinated approach aimed at the detection and mitigation of the threat posed by IEDs. In the context of the War on Terror, it seeks to disrupt IED related terrorist activities, safeguard critical infrastructure and civilians. It combines threat assessment and specialist explosive hazard response, and coordinated intelligence to prevent IED attacks, for there to be a disruption within terrorist networks and material damage to maintain operational continuity.

5) USA Patriot Act:

The Act was first introduced in the 2001s, post September 9th attacks, which declared counter attacks and future course of action. The heart of the Act was to strengthen national security and intelligence agencies. A key part of the act was Section 215, which allowed federal law enforcement to apply for Foreign Intelligence Surveillance Court (FISC) orders to compel the production of institutional records relevant to a counterterrorism investigation. This was

considered highly controversial from other nations for it included secret monitoring.

6) Black Sites:

Black sites were unacknowledged detention facilities operated by the CIA on foreign soil. They formed the physical infrastructure of the "Extraordinary Rendition" program, acting as lawless geographic vacuum chambers. The detainees had to undergo acts of high level terror. Within these sites, detainees were subjected to the EITs without any public record of their existence or location. These acts however gained criticism soon enough, as the black sites were considered to strip the detainees of all sorts of human rights. The violation of UN is very evident here. Under Articles 55 and 56 of the UN Charter, all member states pledge themselves to take joint and separate action to promote "universal respect for, and observance of, human rights and fundamental freedoms for all."

7) EITs:

Enhanced Interrogation Techniques (EITs) were a system of state sanctioned physical and psychological coercion methods developed by the CIA following the September 11 attacks, which were meant to be merely against the perpetrators in the 9/11 attacks, however, the 2014 Senate Intelligence Committee Report explicitly revealed that out of 119 known individuals detained by the CIA, at least 26 (more than 20%) did not meet the legal standard for detention, with many being cases of mistaken identity, faulty intelligence, or bad bounties. The EIT is considered to be a direct violation of the Geneva Convention's Articles and a clear violation of the foundation of all international law.

Sub Topic #2: The Weaponization of Under Sea Infrastructure

1) Keyterms and Definition:

A. *Undersea Infrastructure:*

There is no single comprehensive UN definition of “undersea infrastructure.” In international practice, the term generally encompasses physical infrastructure located beneath or on the seabed that provides communications, energy, transport, surveillance or other strategic services. This includes submarine telecommunications cables, electricity interconnectors, oil and gas pipelines, offshore energy installations and certain seabed monitoring systems.

The distinction between civilian and military infrastructure is increasingly difficult because the same seabed environment can contain privately owned telecommunications cables alongside State owned energy infrastructure and military surveillance systems. A telecommunications cable may be civilian in ownership but also important to national security because of the volume of international communications carried through it.

NATO has estimated that more than 95% of global internet traffic travels through undersea cables and that approximately 1.3 million kilometres of submarine cables support an estimated US\$10 trillion in financial transactions every day. These figures are a clear example of why the physical destruction of infrastructure that may appear commercially private can have consequences extending into national and international security.

B. *Critical Infrastructure:*

There is no universally binding UN treaty definition of “critical infrastructure” specifically for submarine systems. The term is generally used for infrastructure whose disruption could seriously affect essential societal, economic or governmental functions. The distinction is important because not every undersea

structure is automatically critical infrastructure. A cable carrying high volumes of international communications or connecting an isolated population is different from infrastructure whose failure has limited consequences.

C. Weaponization:

Weaponization can be understood as the deliberate exploitation, disruption, manipulation or militarisation of undersea infrastructure or its surrounding environment to obtain a strategic, coercive, intelligence or security advantage.

2) Why Has Undersea Infrastructure Become a Security Issue?

Modern undersea infrastructure combines three characteristics that make it particularly sensitive, which is that it is physically vulnerable, difficult to monitor continuously and essential to highly interconnected economies.

Submarine cables are particularly important because internet communications are not primarily dependent on satellites. NATO has stated that more than 95% of internet traffic is transmitted through undersea cables. The enormous geographical length of these networks means that a cable can pass through several maritime jurisdictions and international waters before reaching its landing station.

The International Cable Protection Committee has also emphasized that most cable damage is not necessarily caused by hostile activity. Around 70% of cable faults are associated with fishing activity and ship anchors, demonstrating why an unexplained break cannot automatically be classified as an attack. This distinction becomes central when attribution is politically contested.

3) Context:

A. 1858 Early Submarine Communications:

The first successful transatlantic telegraph cable was completed in 1858 which established the basic principle that information could depend upon physical infrastructure crossing the seabed. Although the technology was primitive compared with modern fibre optic systems, the vulnerability was already present,

because destroying a physical communications line could interrupt communication between distant territories.

During the First World War, submarine communications infrastructure became quite relevant to military operations because states attempted to interrupt enemy communications while protecting their own networks. During the Second World War, the importance of underwater communications expanded further alongside submarine warfare and naval intelligence.

B. Cold War:

The Cold War transformed the seabed from a communications environment into an important military intelligence domain. One of the most significant developments was the United States' Sound Surveillance System (SOSUS). Developed during the Cold War, SOSUS used underwater acoustic sensors to detect and track submarines over long distances. Its principal strategic purpose was monitoring Soviet submarine activity, particularly submarines capable of threatening NATO and North American security.

This development created an early version of a problem now seen with modern seabed sensors and autonomous systems which is that the same physical environment can support civilian infrastructure, scientific activity and military surveillance simultaneously.

C. 1970, UN General Assembly Resolution 2749:

Before UNCLOS was concluded, the General Assembly adopted Resolution 2749 (XXV) on 17 December 1970, entitled the Declaration of Principles Governing the Seabed and the Ocean Floor, and the Subsoil Thereof, beyond the Limits of National Jurisdiction.

The resolution received 108 votes in favour, 0 against and 14 abstentions. It declared that the seabed and ocean floor beyond national jurisdiction and their resources constitute an area to be used for peaceful purposes and in the interests of mankind.

However, Resolution 2749 was a General Assembly declaration rather than a Security Council enforcement regime. It therefore did not establish a mechanism

through which the Council could investigate or prevent every military activity occurring on the seabed.

D. 1971 1972, Seabed Arms Control Treaty:

The Cold War produced the first major treaty specifically restricting the emplacement of weapons on the seabed.

The full title is the Treaty on the Prohibition of the Emplacement of nuclear weapons and Other Weapons of Mass Destruction on the Sea Bed and the Ocean Floor and in the Subsoil Thereof.

It was opened for signature on 11 February 1971 and entered into force on 18 May 1972. The General Assembly had previously adopted Resolution 2660 (XXV) on 7 December 1970, transmitting the treaty for signature.

The treaty prohibits States Parties from placing nuclear weapons or other weapons of mass destruction, or structures designed to store, test or deploy such weapons, on the seabed and ocean floor beyond the 12 nautical mile zone specified by the treaty.

The treaty does not constitute a prohibition on seabed militarisation.

It does not prohibit all:

- ★ Conventional military activity;
- ★ Submarines;
- ★ Sonar;
- ★ Military surveillance;
- ★ Conventional seabed sensors;
- ★ Military exercises.

E. UNCLOS:

The United Nations Convention on the Law of the Sea (UNCLOS) was adopted on 10 December 1982 and entered into force on 16 November 1994.

UNCLOS is the central legal framework for determining what States may do in different maritime zones. It does not establish a general prohibition on military activity at sea. Instead, it distributes different rights and jurisdiction among coastal States, flag States and other States depending upon geographical location.

The United Nations Convention on the Law of the Sea (UNCLOS) is the most important legal framework for understanding almost every dispute involving undersea infrastructure. It was adopted on 10 December 1982 and entered into force on 16 November 1994. UNCLOS is sometimes described as the “constitution for the oceans” because it establishes the legal status of maritime zones, the rights and duties of coastal States, the freedoms of other States, rules for marine environmental protection, navigation, scientific research, seabed resources and submarine cables and pipelines.

The legal status of an undersea installation depends heavily on where it is located. A foreign military submarine operating 8 nautical miles from a coastline is operating under a very different legal regime from a submarine operating 80 nautical miles offshore. Similarly, a telecommunications cable passing through a State's EEZ does not give that State the same rights over the cable that it would have over infrastructure lying within its territorial sea.

UNCLOS divides the maritime environment into different legal zones. These zones represent different distributions of sovereignty, jurisdiction and freedom.

Territorial Sea, Notable UNCLOS articles:

- a. Under Article 3, every State has the right to establish a territorial sea extending up to 12 nautical miles from its baselines.
- b. Under Article 2, the sovereignty of the coastal State extends to the territorial sea, including its:

- ★ Water column;
- ★ Airspace;
- ★ Seabed;
- ★ Subsoil.

Within the territorial sea, the coastal State exercises sovereignty, although that sovereignty is subject to certain limitations imposed by international law, most importantly, the right of innocent passage.

- c. Article 17 gives ships of all States the right of innocent passage through the territorial sea.
- d. Article 19 provides a list of activities that make passage prejudicial to the peace, good order or security of the coastal State. These include activities

The UNCLOS states that if every coastal State could completely prohibit foreign ships from passing through its territorial sea, international navigation would become extremely difficult. Maritime trade routes would effectively depend on the permission of individual coastal States.

Threat or use of force;

- ★ Weapons exercises;
 - ★ Intelligence gathering prejudicial to the defence or security of the coastal state;
 - ★ Launching or taking on board military aircraft;
 - ★ Launching military devices;
 - ★ Willful and serious pollution;
 - ★ Fishing;
 - ★ Certain research or survey activities.
- e. A foreign submarine passing through another State's territorial sea while submerged raises a separate problem because of Article 20, which provides that “In the territorial sea, submarines and other underwater vehicles are required to navigate on the surface and to show their flag.”
 - f. Under Article 33, the coastal State may exercise the control necessary to prevent or punish infringement of its:

- ★ Customs laws;
- ★ Fiscal laws;
- ★ Immigration laws;
- ★ Sanitary laws.

Article 19 provides a list of activities that make passage prejudicial to the peace, good order or security of the coastal State. These include activities such as:

- ★ Weapons exercises;
- ★ Intelligence gathering prejudicial to the defence or security of the coastal State;
- ★ Launching or taking on board military aircraft;
- ★ Launching military devices;
- ★ Willful and serious pollution;
- ★ Fishing;
- ★ Certain research or survey activities.

A foreign submarine passing through another State's territorial sea while submerged raises a separate problem because of Article 20, which provides that “In the territorial sea, submarines and other underwater vehicles are required to navigate on the surface and to show their flag.”

Under Article 33, the coastal State may exercise the control necessary to prevent or punish infringement of its:

- ★ Customs laws;
- ★ Fiscal laws;
- ★ Immigration laws;
- ★ Sanitary laws.

This means that the contiguous zone does not generally give a State broad authority to regulate foreign military activity simply because a vessel is operating there.

The Exclusive Economic Zone, or EEZ, can extend up to 200 nautical miles from the baselines under Article 57. However, An EEZ is not sovereign territory. Instead, Article 56 grants the coastal State specific sovereign rights and jurisdiction.

These include sovereign rights for:

- ★ exploring natural resources;
- ★ exploiting natural resources;
- ★ conserving natural resources;
- ★ managing natural resources;
- ★ producing energy from water, currents and winds.

The coastal State also has jurisdiction over certain matters including:

- ★ artificial islands and installations;
- ★ marine scientific research;
- ★ protection and preservation of the marine environment.

Under Article 58, other States retain important freedoms, including:
freedom of navigation;

- ★ freedom of overflight;
- ★ laying submarine cables and pipelines;
- ★ other internationally lawful uses of the sea related to these freedoms.

They must, however, exercise these freedoms with due regard for the rights and duties of the coastal State.

4) **Baltic Sentry:**

- A. Baltic Sentry is a NATO maritime activity launched on 14 January 2025 following a series of incidents involving undersea telecommunications and energy infrastructure in the Baltic Sea. It is significant because it is one of the best examples of a military alliance treating civilian undersea infrastructure as a

security concern. It is important because it contains dense concentrations of submarine telecommunications cables, electricity interconnectors, gas pipelines, offshore energy infrastructure, commercial shipping routes, NATO's military forces and Russian maritime activity. It uses a combination of:

- ★ Frigates;
- ★ maritime patrol aircraft;
- ★ naval drones;
- ★ national surveillance capabilities;

Baltic Sentry subsequently became a testing ground for autonomous maritime technology. Task Force X Baltic, launched in January 2025, supported Baltic Sentry by testing autonomous systems and AI enabled technologies. Between March and October 2025, approximately 70 air and maritime drones were deployed and tested alongside Allied maritime assets. It was reported by NATO that these systems improved situational awareness and the detection of potentially malicious activity. Nato also developed Mainsail, which is a data fusion system combining information from satellite imagery, sonar and underwater sensors. Its purpose is to produce "seabed to space" situational awareness and identify patterns in maritime activity.

5) AUKUS and the Undersea domain

- A. AUKUS is a security partnership between Australia, the United Kingdom and the United States, established in September 2021. Its relevance to the undersea domain is particularly strong because both of its pillars contribute to the development of advanced underwater capabilities.

B. *Pillar I, Nuclear powered submarines:*

It concerns Australia's acquisition of conventionally armed, nuclear powered submarines. Nuclear powered submarines have significantly greater endurance than conventionally powered submarines because they do not depend upon frequent refuelling. Their value therefore includes:

- ★ Longer duration underwater operations;
 - ★ Greater range;
 - ★ Enhanced stealth;
 - ★ Anti submarine warfare;
 - ★ Intelligence, surveillance and reconnaissance;
- Protection of maritime approaches.

As of the 30 May 2026 AUKUS ministerial statement, the partners confirmed progress toward Australia's nuclear powered submarine capability and arrangements for the Submarine Rotational Force West, with U.S. and UK submarine presence associated with HMAS Stirling in Western Australia. It was also outlined by Australia that major infrastructure investments connected with the programme.

C. Pillar II, Advanced undersea technology:

On 30 May 2026, AUKUS announced its first Pillar II Signature Project, concerning Uncrewed Undersea Vehicles (UUVs). Delivery is scheduled to begin in 2027. The project is intended to support surveillance, reconnaissance, critical seabed infrastructure protection, anti submarine warfare, anti surface warfare, mine countermeasures, electronic warfare, contested littoral operations, and logistics. The systems are intended to operate alongside crewed vessels and submarines and to increase interoperability through common standards, operational concepts and control systems.

Traditional naval systems are relatively visible. A submarine or surface vessel is associated with a State, has identifiable markings and normally operates under an identifiable chain of command. But a UUV is different, An autonomous or remotely operated vehicle may:

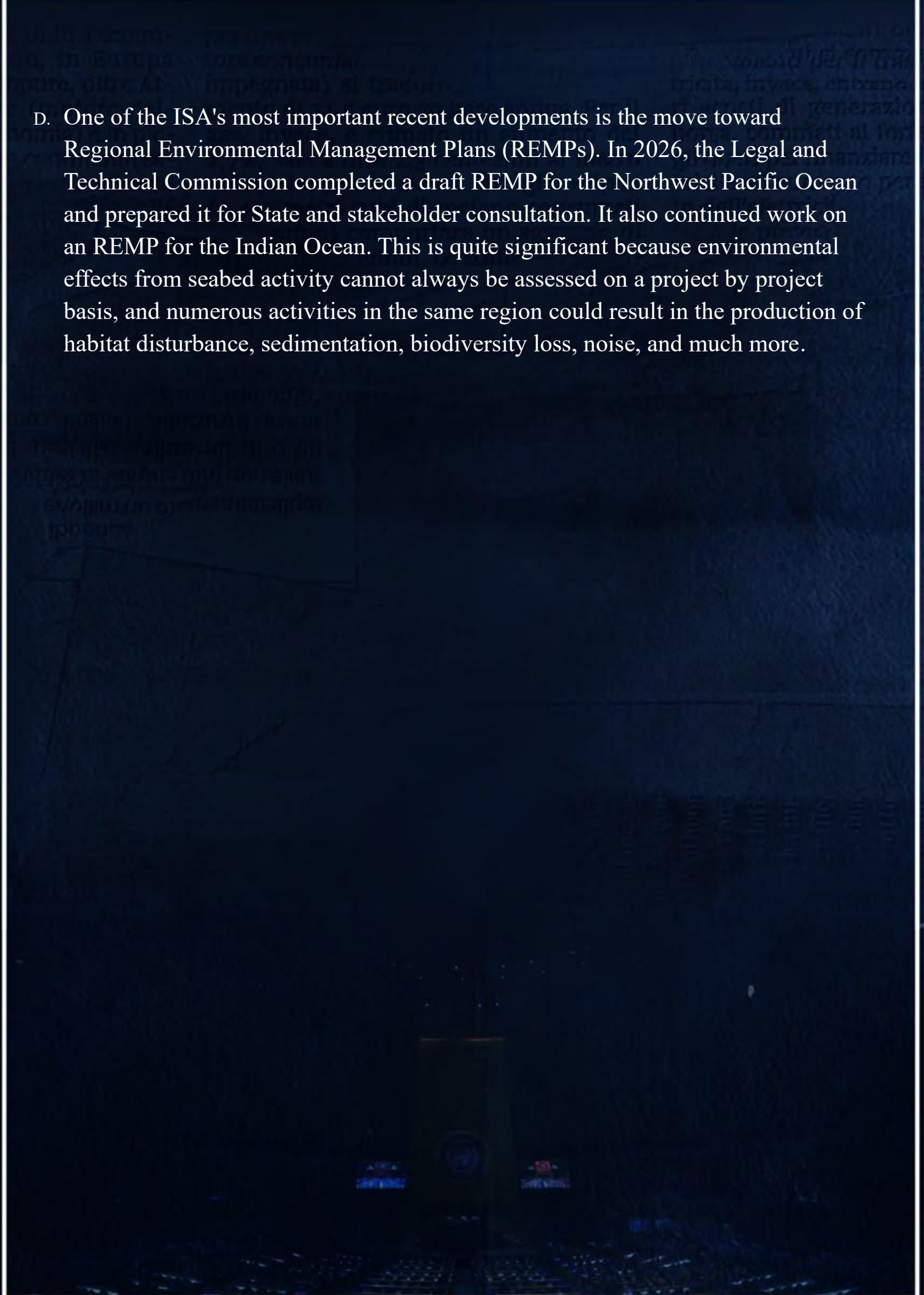
- ★ Remain underwater for extended periods;
- ★ Operate close to infrastructure;
- ★ Collect information without a large visible platform;

- ★ Interact with other autonomous systems; ★ perform surveillance without an onboard crew.

6) **International Seabed Authority:**

- The International Seabed Authority (ISA) was established under UNCLOS to organize and control mineral related activities in the Area, meaning the seabed and ocean floor beyond national jurisdiction. The ISA has been developing a regulatory framework for the exploitation of mineral resources in the Area since 2014. The proposed Exploitation Regulations, often referred to as part of the Mining Code, are intended to establish rules governing future commercial exploitation of deep sea minerals. The regulations address issues including environmental protection, exploitation contracts, compliance, inspection, monitoring, financial arrangements, closure plans, liability, and emergency procedures.
- During the ISA's 31st session in 2026, a Friends of the President group was working specifically on submarine cable protection, including proposals concerning draft regulations relevant to activities in the Area. This is important because deep sea mining and submarine infrastructure can occupy the same seabed. A mining operation could potentially cross or approach a cable route, interfere with maintenance access, generate sediment plumes, physically disturb the seabed, and create risks for existing infrastructure.
- One of the ISA's most important recent developments is the move toward Regional Environmental Management Plans (REMPs). In 2026, the Legal and Technical Commission completed a draft REMP for the Northwest Pacific Ocean and prepared it for State and stakeholder consultation. It also continued work on an REMP for the Indian Ocean. This is quite significant because environmental effects from seabed activity cannot always be assessed on a project by project basis, and numerous activities in the same region could result in the production of habitat disturbance, sedimentation, biodiversity loss, noise, and much more.

D. One of the ISA's most important recent developments is the move toward Regional Environmental Management Plans (REMPs). In 2026, the Legal and Technical Commission completed a draft REMP for the Northwest Pacific Ocean and prepared it for State and stakeholder consultation. It also continued work on an REMP for the Indian Ocean. This is quite significant because environmental effects from seabed activity cannot always be assessed on a project by project basis, and numerous activities in the same region could result in the production of habitat disturbance, sedimentation, biodiversity loss, noise, and much more.



7) **Acoustic Colonisation:**

Acoustic colonisation can describe the progressive establishment of persistent influence over the underwater acoustic environment through sonar, hydrophones, seabed acoustic sensors, underwater surveillance networks, acoustic monitoring systems, and autonomous underwater vehicles. The concept is that control of the acoustic environment can provide knowledge about submarine movements, vessel traffic, infrastructure activity, seabed conditions, and underwater communications.

Arctic Race and Polar Undersea Militarisation

- A. The Arctic has become a significant area of competition due to changing sea ice conditions, increased accessibility, resource potential, emerging maritime routes and the growing military importance of the High North. The eight Arctic States are Canada, Denmark (through Greenland), Finland, Iceland, Norway, Russia, Sweden and the United States, while the five States bordering the Arctic Ocean are Canada, Denmark/Greenland, Norway, Russia and the United States. Arctic competition is not legally equivalent to territorial competition over an ungoverned region.

Maritime jurisdiction, navigation and seabed rights are principally governed by the United Nations Convention on the Law of the Sea (UNCLOS), while the UN Charter regulates the use of force. UNCLOS Articles 76 and 77 establish the legal framework for continental shelf rights, including the possibility of an extended continental shelf beyond 200 nautical miles where the relevant geological and geographical requirements are satisfied. These rights concern the seabed and subsoil and do not constitute sovereignty over the waters above them; Article 78 expressly preserves the legal status of the superjacent waters and the freedoms and rights of other States. The Commission on the Limits of the Continental Shelf (CLCS) assesses the scientific basis for outer continental shelf claims, but its recommendations do not themselves determine maritime boundaries between States.

B. *Arctic Seabed Militarization:*

Arctic militarisation involves capabilities operating beneath the surface, including submarines, fixed acoustic sensors, seabed surveillance systems, remotely operated vehicles and autonomous underwater vehicles. The strategic importance of these systems derives partly from the Arctic's connection to the North Atlantic, the North Pacific and major military reinforcement routes. Underwater infrastructure, including telecommunications cables and energy installations, is also becoming increasingly relevant because disruption or surveillance of such infrastructure could affect civilian communications, economic activity and military operations. NATO's Arctic security posture has expanded significantly, particularly following the accession of Finland and Sweden. In February 2026, NATO launched Arctic Sentry, a multi domain activity designed to strengthen Allied deterrence and defence in the Arctic and High North. The operation is led by Joint Force Command Norfolk and coordinates with NATO and North American commands including NORAD, US Northern Command and US European Command. NATO has identified sea lines of communication, reinforcement routes and increased Russian military activity as important elements of the Arctic security environment.

c. *Autonomous and Underwater Surveillance Systems:*

The deployment of autonomous and remotely operated systems is changing the nature of Arctic undersea surveillance. In June 2026, NATO launched Task Force X Arctic, building upon its earlier Task Force X Baltic programme. The initiative employs networked uncrewed systems under ultimate human control to develop persistent multi domain situational awareness across the Arctic, High North and North Atlantic. Similar technologies can be applied to monitoring submarine activity, detecting unusual activity around critical infrastructure, mapping the seabed and maintaining persistent surveillance in areas where conventional patrols are difficult or expensive. The development of these systems creates legal questions concerning jurisdiction, attribution and the status of autonomous underwater vehicles. UNCLOS contains rules governing submarines and underwater vehicles in territorial seas, navigation and activities in maritime zones, but it does not contain a comprehensive regime specifically regulating modern autonomous military underwater systems. Their legality therefore depends on the maritime zone concerned, the purpose and conduct of the operation, its effects and the rights of the coastal State and other States.

D. *Environmental and Acoustic Implications:*

Undersea militarisation also has environmental implications because military sonar, seabed sensors, shipping and other activities can alter marine acoustic environments. Arctic waters are particularly relevant because many areas historically experienced relatively low levels of anthropogenic underwater noise. UNCLOS Articles 192 and 194 establish obligations to protect and preserve the marine environment and to prevent, reduce and control pollution, while Article 206 requires environmental assessment where activities may cause substantial pollution or significant and harmful changes to the marine environment. Underwater noise is not automatically classified as unlawful pollution, and international law does not impose a general prohibition on military sonar. However, activities that produce significant environmental harm may engage broader environmental obligations. The International Maritime Organization has also developed guidelines addressing underwater radiated noise from commercial shipping, although these guidelines expressly do not establish equivalent rules governing warships or deliberate military sonar operations.

E. *Arctic Continental Shelf Claims:*

Russia's continental shelf submissions provide a major legal precedent for Arctic seabed competition. Russia initially submitted information concerning its Arctic continental shelf to the CLCS in 2001 and subsequently submitted a revised submission in 2015, followed by further information in later years. The CLCS adopted recommendations concerning Russia's revised Arctic submission in 2023. Russia subsequently submitted additional information concerning the Gakkel Ridge in October 2023, followed by an amended executive summary in March 2026.

The process demonstrates that competing Arctic seabed claims are addressed through the scientific and legal procedures established by UNCLOS rather than through military occupation. Importantly, a CLCS recommendation concerning the outer limit of a continental shelf does not itself resolve overlapping maritime boundaries between States. Where boundaries overlap, the relevant States must resolve the delimitation separately through agreement or another applicable peaceful mechanism.

F. Cold War Precedent:

The Cold War provides an important precedent for large scale undersea surveillance in the Arctic and North Atlantic. The United States and its allies developed the Sound Surveillance System (SOSUS), a network of fixed underwater acoustic sensors designed primarily to detect and track Soviet submarines. The system demonstrated the strategic value of persistent seabed based acoustic surveillance and contributed to anti submarine warfare throughout the Cold War. Modern autonomous underwater systems and distributed seabed sensors represent technological developments of the same broader surveillance concept, although their capabilities, legal context and operational characteristics are substantially different. SOSUS therefore constitutes a strategic precedent rather than a direct legal precedent.

G. Legal Limits on Polar Militarisation:

There is no general rule of international law declaring the Arctic a demilitarised zone. Military activities remain subject to the UN Charter, UNCLOS and other applicable international agreements. The 1971 Seabed Arms Control Treaty prohibits the emplacement of nuclear weapons and other weapons of mass destruction on the seabed and ocean floor beyond the outer limit of the territorial sea, but it does not prohibit conventional submarines, acoustic surveillance, military sensors or every form of seabed military activity. UNCLOS additionally establishes different rights and restrictions depending on whether an activity occurs in the territorial sea, exclusive economic zone, continental shelf or areas beyond national jurisdiction. Consequently, the presence of military forces or surveillance systems in the Arctic is not, by itself, unlawful. The legal assessment depends upon the specific activity, its location, its purpose, its effects and whether it interferes with the rights or jurisdiction of another State.

9) Important Case Studies:

A. Nord Stream Explosions, 2022:

On 26 September 2022, a series of underwater explosions damaged the Nord Stream 1 and Nord Stream 2 natural gas pipelines in the Baltic Sea, producing major gas leaks in the vicinity of the Danish island of Bornholm and Sweden. The pipelines were commercial energy infrastructure located on the seabed and, although not operational in the same manner at the time of the explosions, remained significant links between Russia and Europe. Denmark, Sweden and Germany initiated separate investigations into the incident, while Sweden subsequently closed its investigation in February 2024 without publicly attributing responsibility. The incident demonstrated the vulnerability of fixed seabed infrastructure to deliberate physical attack and created a major attribution problem because the infrastructure was in international waters while falling within the maritime jurisdictions and security interests of several States. It also demonstrated the difficulty of applying existing international law to covert attacks against infrastructure: the legal consequences depend on attribution, the applicable maritime jurisdiction and whether the conduct is characterised as sabotage, unlawful use of force or an act triggering the international responsibility of a State.

B. Balticconnector, 2023:

On 8 October 2023, the Balticconnector gas pipeline linking Finland and Estonia was damaged in the Baltic Sea, simultaneously with damage to telecommunications cables connecting Finland and Estonia. Finnish authorities subsequently identified the Hong Kong flagged container vessel Newnew Polar Bear as having passed through the relevant area and stated that an external force had caused the pipeline damage. Finnish investigators later concluded that the vessel's anchor had caused the damage, while the investigation into responsibility and the circumstances surrounding the incident continued. The case is significant because it illustrates the evidentiary difficulty of distinguishing accidental infrastructure damage from deliberate interference. Unlike a conventional military attack, damage to a submarine pipeline can initially present as a maritime accident and require vessel tracking, seabed examination, physical

evidence and international cooperation before responsibility can be established. It therefore demonstrates the importance of attribution mechanisms in determining whether an undersea infrastructure incident constitutes an accident, criminal act or State linked operation.

C. Baltic Sea Telecommunications Cable Incidents, 2024–2025:

A series of incidents involving submarine telecommunications and energy infrastructure in the Baltic Sea during 2024 and early 2025 increased European concern regarding the vulnerability of critical undersea infrastructure. In December 2024, the telecommunications cables connecting Finland Germany and Lithuania Sweden were damaged, while Estonia Finland infrastructure had also experienced damage in the preceding period. The incidents prompted increased maritime monitoring and cooperation between NATO members. In January 2025, NATO established Baltic Sentry, deploying frigates, maritime patrol aircraft, naval drones and national surveillance capabilities to strengthen protection of critical undersea infrastructure. The significance of these incidents lies in the transition from individual infrastructure failures to a broader security problem involving persistent surveillance, maritime attribution and protection of strategically important seabed systems. They also established a precedent for NATO treating the protection of civilian undersea infrastructure as a collective security concern without automatically classifying every incident as an armed attack.

D. AUKUS Underwater Uncrewed Vehicles, 2026:

AUKUS is a contemporary example of the integration of advanced underwater technology into military planning and critical infrastructure protection. In May 2026, Australia, the United Kingdom and the United States announced their first AUKUS Pillar II Signature Project focused on underwater uncrewed vehicle payloads and enabling systems, with delivery beginning in 2027. The project is intended to support surveillance and reconnaissance, protection of critical national seabed infrastructure, anti submarine and anti surface warfare, mine countermeasures, electronic warfare and other maritime operations. Its significance to the weaponization of undersea infrastructure lies in the dual use character of underwater systems: the same technologies capable of monitoring and protecting cables and seabed installations can also provide persistent

surveillance or military capabilities in their vicinity. AUKUS itself does not establish a new international legal regime, and the legality of individual operations remains governed by existing international law, including UNCLOS and the UN Charter.



Sub-Topic #3: Quantum Espionage

Quantum Espionage is a cutting-edge technology, under the umbrella of Cyber Intelligence, which primarily uses Quantum Mechanics and Quantum Computing to decrypt or intercept data.

The new technology has gained attention from all nations present on top of the global politics hierarchy. The United States and China especially are at the forefront of a race to build the world's first quantum machine, and whoever crosses the finish line first will attain global dominance for generations to come.

Key Terms and Definitions:

1. *Quantum Hegemony:*

The dominance of a nation in the context of deployment of advanced technology is referred to as Quantum Hegemony, allowing the state to gain disproportionate military, intelligence and economic advantages over its rival power. Contextually, China and the United States stand at the top of technological hierarchy which may exacerbate acceleration of military and nuclear preparations.

2. *Post Quantum Cryptography (PQC)*

The technology is designed to resist quantum computers originating attack, to protect governmental, military based networks and sensitive information from being attacked from any future quantum threats referred to as PQC.

3. *Quantum Sensing:*

The usage of quantum intelligence to develop highly sensitive instruments which have the ability to detect changes in gravity or magnetic fields within a very limited amount of time. In the context of military and intelligence applications, the sensors can also potentially improve submarine detection, enable navigation without GPS and help with identification of covert underground structures.

4. *Harvest now, Decrypt Later:*

A cyber intelligence strategy in which state sponsored actors intercept and store encrypted data with the intention of decrypting it once sufficiently advanced quantum computers become available. This poses a significant long-term security threat, as sensitive diplomatic communications, military intelligence, and classified government information could be exposed years after collection.

The Promises and Threats of Quantum Technologies:

Quantum computing could be easily manipulated to break pre-quantum encryption, such as public key cryptography (PKC). When this is further combined with cyber infiltration capabilities, it leaves room for threat which extends to cryptocurrencies and blockchain systems, it is important to note that these very systems too rely on the same vulnerable encryption standards.

- 1) Due to their superior mastery over handling complex probabilistic scenarios more efficiently than classical computers, quantum computers can be considered to be excellent source to predict different geopolitical and economic variables where a conflict might occur.
- 2) The technology also promises to provide breakthrough in scientific fields and aid in complex biological processes like Protein folding, drug discovery, and biomaterials science. Quantum computers may also be integrated with classical supercomputers, which could potentially process power and speed greater than any supercomputer could provide alone. Quantum science unlocks advances and leaves room for interception in military applications including battle planning, weaponry, and command, control, and communications.

Espionage Incidents:

Despite being an emerging technology, no nation has actively and outrightly been exploiting its benefits during warfare. However, a plethora of reports exist which testify to the advancements taking place by nations in the field of Quantum Intelligence.

a. United states:

The U.S. government has launched ambitious programs to maintain leadership in quantum computing. Central to this effort is the National Quantum Initiative Act (NQI Act) of 2018.

This Act mandates a coordinated multiagency program to advance quantum information science, spanning the National Institute of Standards and Technology (NIST), the Department of Energy (DOE) and other agencies. In practical terms, the NQI Act set in motion significant funding and organizational resources to turbocharge quantum R&D. For example, it called for creating between 4 and 10 new Quantum Information Science Research Centers, competitively awarded and multidisciplinary in nature.

b. China:

- 1) In mid-2019, the FBI issued a public warning that foreign intelligence agents were actively recruiting students and professors at U.S. universities to obtain emerging technology research. This warning followed incidents of suspicious approaches and offered incentives to researchers in fields like quantum information science. It reflected awareness that Beijing's and Moscow's intelligence services often use informal collectors in addition to hackers. The FBI alert was meant to harden academia against such espionage, which often goes unreported, a point underscored by FBI Directors.
- 2) Chinese state-backed hacker groups have been caught infiltrating a wide array of companies and labs to steal intellectual property. Dutch intelligence revealed in 2024 that a Chinese cyber campaign had breached "dozens" of Western government and industry networks. U.S. officials likewise attest that China is running a "well-resourced and systematic campaign" to acquire quantum innovations by any means, including illicit transfer via insiders, cyber intrusions, and front companies.

c. Russia:

- 1) Recent U.S. indictments have exposed Russian “procurement front” networks that illicitly acquired advanced Western technologies for Moscow’s intelligence and military agencies. One 2022 case targeted Serniya Engineering and Sertal LLC, a Moscow-based shell company network that smuggled highly regulated electronics and sophisticated testing equipment (including quantum computing components) to Russian state end-users. According to the indictment, the Serniya/Sertal operation was directed by Russian intelligence and obtained dual-use tech for clients like Russia’s Ministry of Defense, the SVR (Foreign Intelligence Service), and components of the FSB.
- 2) Throughout the last ten years, Russian state-backed hacking units increasingly targeted Western quantum programs through cyber espionage. Intelligence reports (later declassified in part) noted that Russian hackers had breached or probed U.S. university networks to steal classified quantum encryption research. Institutions such as the University of Maryland’s Joint Quantum Institute and the Chicago Quantum Exchange were flagged by U.S. agencies as “high risk targets” after detecting intrusion attempts linked to Russian actors.

d. Iran and North Korea via Singapore/Japan (2021):

A procurement network based in Singapore and Japan (Singapore affiliate of Chinese Corad Technology) was sanctioned by the U.S. for covertly acquiring and exporting quantum-related technologies to adversaries. The firm acted as a front company to funnel Western tech (including quantum computing components) to Iran’s military, North Korean fronts, and Chinese defense entities.

e. France and Iran:

A French company, Cryostar SAS, illicitly supplied ultra-cold technology to Iran in violation of export laws. Cryostar pleaded guilty to conspiring to export cryogenic submersible pumps to Iran without a license. Such pumps, which achieve extremely low temperatures, have applications ranging from rocket launch systems to superconducting quantum equipment.

f. The Wassenaar Agreement:

The Wassenaar Arrangement Governments may decide to impose export controls on a certain technology, or groups of technologies against one or several countries, or they can join an export controls organisation or treaty, such as the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.

Quantum falls under The Wassenaar Arrangement, established on 12 July 1996, in Wassenaar, Netherlands. It was established to contribute to regional and international security and stability by promoting transparency and greater responsibility in transfers of conventional arms and dual use goods and technologies, thus preventing destabilizing accumulations. Participating states seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals and are not diverted to support such capabilities.

Relevant UN articles:

1) A/RES/53/70 (1998):

A/RES/53/70 is a foundational document for discussing quantum espionage within international information security. The resolution recognizes that information technologies can be exploited in ways that harm international stability and the security of States, and specifically raises concerns over unauthorized interference with information systems. In the context of quantum espionage, its principles can be extended to the future interception or decryption of protected state communications and the targeting of sensitive information infrastructure using quantum capabilities. It also encourages international consideration of emerging information and security threats, making its framework applicable to risks that were not yet fully developed when the resolution was adopted.

2) A/RES/71/28 (2016)

This resolution establishes the connection between State Security and emerging technologies which can potentially threaten both Cyber and Physical Infrastructures. The resolution concludes the application of the UN Charter upon States' usage of information technologies. This means that all future actions whether be quantum enabled interception, cryptographic compromise or cyber destruction will still be held accountable and will be bound under the already existing International Legal Framework

3) A/RES/73/266 (2018) :

The resolution established a group of Governmental Experts to investigate the responsible State behaviour in the application of international law, pertaining to Cyber Activities. Its relevance to quantum espionage lies in establishing standards prior to large scale widespread technological capabilities. Cyber operations enabled by Quantum could eventually challenge existing expectations concerning state responsibility and critical infrastructure alongside intelligence activities. The framework created through this UN process therefore provides delegates with a basis for discussing whether existing cyber principles are adequate for quantum capabilities or whether the introduction of additional international rules will eventually be required.