Main MUN conference

Main Model United Nations Conference
Frankfurt am Main, Germany
22nd Session
26th of February to 1st of March 2026

Daring Democracy

# Background Guide

## Security Council

Written by: Alissa Lingnau and Phil Kievel

www.mainmun.de

# Table of Contents

# 1. Words of Welcome

Dear honorable delegates,

it is our utmost pleasure to welcome you to MainMUN 2026, to Goethe-University, and to “the heart of Europe”, to Frankfurt am Main. We are very much looking forward to spending four days full of fruitful debates, inspiring personal exchanges, and exciting encounters with you. Of course, working in a formal session, lobbying, negotiating a compromise, and passing resolutions will only be one aspect of your experience at MainMUN. After your diplomatic work is done for the day, you will be able to benefit from a rich academic and, above all, social program. MUNs are an exhilarating opportunity to broaden your horizons, step out of your comfort zone, develop empathy for others' points of view while passionately representing your own, and, more than anything, meet and socialize with open-minded, smart, and fun people from all over the world. It's up to you how you want to seize this wonderful opportunity to take part in one of Germany's biggest MUNs. We, your Chairs, are always available to you and will be very happy to advise, support, and assist you.

A little bit about us:

Hi, my name is Alissa, and my MUN journey began with MainMUN 2023, where I was part of the organizing team. Inspired by this experience, I went on to participate in several MUN conferences across Germany and have since chaired the ECOSOC committee at MainMUN 2024 and the UNSC at MainMUN 2025. This year marks my second time chairing the UNSC at MainMUN, once again together with Phil, after we already chaired the committee as a team last year. Despite my chairing experience, I still genuinely enjoy being a delegate and most recently participated in the NMUN in New York this April. Academically, I am currently finishing my bachelor’s degree in Political Science and Economics at Goethe University Frankfurt. In addition, I serve as Chair of the MainMUN Foundation e.V., where I am responsible for the legal and financial framework surrounding the conference. Outside MUN and university, you will usually find me working at a consulting firm (mostly from home), at the gym, or doing something creative. I used to be a dancer, which is why I am always open to more unconventional or creative sports. Fun fact: I was born in the United States, but despite that, I somehow ended up with a strong German accent when speaking English.

Hi, dear delegates. I’m Phil, and with years of MUN experience, I am particularly thrilled to be chairing the Security Council together with amazing Alissa this year. I studied law at Goethe University and passed the state exam last year. Currently, I am working as a research assistant at the University, focusing on family law, law of succession, and corporate law. Besides my doctoral thesis that I am currently working on, I’m also participating in an LL.M. program at the University of Vienna. In my free time, you will probably find me out with friends, trying new bars and pubs, at the opera, or at the tennis court.

Here are some things that might be helpful before the conference:

- Read this Background Guide thoroughly and use it as a starting point for your own research,
- Familiarize yourself with your country and its position regarding the discussed topics,
- Have a glance at our rules of procedure,
- Consider preparing a position paper.

We will be there to guide you throughout the conference and are happy to answer any questions that might arise concerning the topic, the conference, your position paper, rules of procedure, or anything else regarding MUN. We are happy that you chose the MainMUN Security Council and look forward to meeting you all in March.

Furthermore, we will be there to guide you in the weeks before the conference, so should you have any questions about the committee or anything else regarding MUN, please feel free to contact us at any time!

- Chair Alissa: alissamarie.lingnau@gmail.com
- Chair Phil: kievel@jur.uni-frankfurt.de

Best wishes, and see you all soon

Alissa & Phil

# 2. About the Committee

## 2.1 Overview

The United Nations Security Council (UNSC) is one of the six principal organs of the United Nations (UN) and is charged with ensuring international peace and security, recommending the admission of new UN members to the General Assembly, and approving any changes to the UN Charter. The UNSC consists of fifteen members, of which five are permanent and have veto power: China, France, the Russian Federation, the United Kingdom, and the United States. The other ten are voted in continental groups by the General Assembly. Each member of the UNSC has one vote. Under the Charter, all Member States of the UN General Assembly must comply with the Council's decisions.

In our simulation of the UNSC, we will take into account the special position of this committee within the United Nations. Therefore, please pay attention to the special rules in the Rules of Procedure.

In addition, there will be double delegations, which means the member states will be represented by two delegates.

## 2.2 History

After the effects of World War II and the failure of the League of Nations, the United Nations were established as an intergovernmental organization to maintain peace and security. In turn, the UNSC was created with the responsibility to maintain those principles. The first session of the UNSC was held on 17 January 1946 at Church House in London, England. Later, however, the UNSC received its permanent domicile at the UN Headquarters in New York. Until 1965, the Security Council compromised five permanent and six non-permanent members. It was after 1965 that the number of non-permanent members was increased to ten. During the Cold War, the UNSC, due to the disagreements between the United States of America and the former Soviet Union, was quite ineffective, and the permanent members made frequent use of their veto power to prevent certain resolutions from passing. The late 1980s, however, were marked by an effective Security Council, which authorized peacekeeping missions in different countries, such as the former Yugoslavia, Somalia, the Democratic Republic of Congo, Kosovo, and East Timor. Since the end of the Cold War, the Council has adopted significantly more resolutions by consensus than during the Cold War.

## 2.3 Competencies

The UNSC is the only body that has the power to adopt binding resolutions. When a resolution is adopted, the member states, in accordance with Article 25 of the Charter of the United Nations (1945), must accept the Council’s decision.

The mandate of the SC is to maintain international peace and security and to take measures whenever those are threatened. The Council's authority is particularly relevant with respect to the UN's four primary purposes, as specified in the Charter of the United Nations (1945): maintaining international peace and security; developing friendly relations among nations; cooperating in solving international problems; promoting respect for human rights, as well as being a center for harmonizing the actions of nations. To prevent the escalation of a given conflict, the Council may call upon the parties to comply with provisional measures. The Council also cooperates with several international and regional organizations, as well as non-governmental organizations, to gather knowledge and implement its decisions.

## 2.4 Operation

The Charter of the United Nations (1945) lays out the Council's specific powers and responsibilities: First, the Council is allowed to call its members to apply sanctions and other measures. Sanctions can, among others, consist of economic and financial penalties, restrictions on travel, or the cancellation of diplomatic relations. Furthermore, the Council has the mandate to investigate any dispute which may lead to aggression between two parties, such as states, other non-state groups, or within national territories. Finally, the Council can decide on military action against any international peace- or security-threatening situation, and, where needed, is allowed to further decide on the deployment of troops or observers. Whether a situation endangers peace or security is determined by the Council.

## 2.5 Special Rules of the Security Council

The right to veto decisions is one of the special rules applied in the SC and sets it apart from the other main bodies of the United Nations. The following rules, in addition to the rules mentioned in the MainMUN Rules of Procedure Guide, will be applied in the SC only.

### 2.5.1 Minimum Majority and Veto Power

Each member of the SC has one vote. Votes on all matters require a majority of nine member states, with the concurrent support or abstention of all permanent members in substantial matters. If one of the five permanent members votes against a matter of substance, such as a draft resolution, it is "vetoed" and does not pass. The five permanent members were granted a special status in the Security Council. Each of them is allowed the right of veto at any time. In accordance with Article 27 of the Charter of the United Nations, "decisions on procedural matters shall be made by an affirmative vote of nine members. "

Decisions of all other matters shall be made by an affirmative vote of nine members, including the concurring votes of the permanent members. If a permanent member does not fully agree with a proposed resolution, but does not want to veto, it may choose to abstain. The resolution can be adopted if the required number of nine favorable votes is given.

### 2.5.2 Declare a Vote Substantial

This is a motion which may only be used by the permanent members of the Security Council. It may be entertained on any procedural motion. The aim of this motion is to change the required vote on the procedural motion into a substantial vote. On a substantial vote, all delegates who are 'present' may abstain, and, even more important, the required majority for that motion to pass is nine, including all permanent members.

Chair: “Are there any points or motions on the floor? N-P5 state, to what point do you rise?”

N-P5 State: “Distinguished chair, we/the Republic of... move(s) to suspend the meeting for the purpose of a caucus for five minutes.”

Chair: “Thank you. This motion is in order at this time. Are there any further motions on the floor? P5 state to what point do you rise?”

P5 state: “Honorable chair, fellow delegates, we/the Republic of... move(s) to declare the motion to suspend the meeting substantial.”

Chair: “This is in order at this time. Is there any opposition to this motion?” (Several placards are raised) “Seeing objections, we will now have to vote upon re-declaring this motion procedural. All those in favor of re-declaring, please raise your placards now.” (12 placards are raised) “Thank you. All those against?” (The P5 state which originally declared the motion substantial raises its placard) “Abstentions?” (Two placards are raised) “Due to the veto of a permanent member state, the motion to re-declare the motion [for suspending the meeting] procedural fails. We will now vote substantially upon suspending the meeting. All those in favor, please raise your placards.” (13 placards are raised) “Against?” (Again, the P5 state, which originally declared the motion substantial, raises its placard) “Abstention?” (One placard is raised) Due to the veto of a permanent member, this motion fails. We will continue with the formal session.

### 2.5.3 Status of Observers

A non-Council member (observer) is given debating rights. This will allow the delegation to be recognized by the Chair during debate and propose motions to the floor or vote upon procedural matters. Observers cannot vote on substantial matters, and submitting draft resolutions or amendments is prohibited. Observers can be UN members whose interests are directly affected, or non-members of the UN and experts, who are invited to the UNSC.

### 2.5.4 Explanation of a Vote

You are allowed to explain your vote after a roll call vote, when you say “no, with rights” or “yes, with rights”. The explanation should be kept rather short, as you will have only a short time to realize it. You may only explain your vote if you vote against a draft resolution or abstain from a vote. Furthermore, you need to remain in diplomatic conduct at all times. Reasons for an explanation of a vote can only refer to your country’s position; personal reasons are not allowed. With voting clause by clause and divisions of the question, it is quite easy to vote in favor only on specific parts of the resolution. To prevent confusion among your colleagues, if you vote against the resolution in a particular case, it might be necessary to explain your vote to the committee. On the other hand, there is, of course, also a possibility to make a final point about the resolution as a whole, but you should be mindful that the chairs will realize if you try to abuse such an explanation.

## 2.6 Bibliography

Bourantonis, D. (2005). The History and Politics of UN Security Council Reform. New York: Routledge.

Encyclopaedia Britannica. (2014): United Nations Security Council. Retrieved from: http://www.britannica.com/EBchecked/topic/532070/United-Nations-Security-Council (19th of January 2023).

United Nations (1945): UN Security Council, What is the Security Council? Article 1 in Charter of the United Nations.

# 3. Introduction to the Topic

"*Critical infrastructures are the backbone of our modern and interconnected economies*" (OECD, 2019, p. 13).

This interdependence became particularly visible following Russia's invasion of Ukraine in 2022. Since the outbreak of the war, Ukraine's energy, telecommunications, and transport infrastructure have been repeatedly targeted through kinetic strikes and cyber operations. These attacks have not only disrupted military logistics but also caused widespread power outages, water shortages, and heating failures for millions of civilians. At the same time, the effects extended beyond Ukraine's borders, contributing to energy price shocks and supply chain disruptions across Europe (Edwards et al., 2025).

This is only one of many regarding interdependencies of critical infrastructures worldwide. Attacks on vital systems go far beyond affecting a nation's government or military operations and have devastating effects on civilian populations (Brown, 2006: 766). In an era of globalization and digitalization, critical infrastructure systems such as energy, communication technologies, transportation, health, and water are increasingly interconnected and mutually dependent. As a result, disruptions in one sector or country can trigger cascading effects across borders, generating economic instability, humanitarian consequences, geopolitical tensions, and declining public trust in state institutions (OECD, 2019: 13). Unlike traditional military targets, modern critical infrastructure is often civilian, digitally operated, and partially privately owned, making it more vulnerable and more difficult to protect. Many contemporary threats further remain largely invisible, occurring in cyberspace or below the threshold of armed conflict (Hern, 2017).

Recognizing the transnational nature of these threats, the United Nations Security Council has increasingly acknowledged critical infrastructure protection as a component of international peace and security. Resolution 2341 (2017) highlights the need for international cooperation to prevent and respond to attacks on critical infrastructure, particularly in the context of terrorism.

Despite its growing relevance, there is no commonly accepted international definition of critical infrastructure. National approaches vary considerably depending on threat perceptions, economic structures, and governance capacities. While sectors such as energy and digital infrastructure are widely recognized as critical, others, including food security, water systems, or education, receive less attention (Laumann et al., 2023: 1). This lack of conceptual alignment complicates international cooperation, limits coordinated risk assessment, and undermines collective resilience. As the OECD (2019: 13) emphasizes, the protection of critical infrastructure cannot stop at national borders, as disruptions increasingly produce transnational spillover effects that demand international responses. These dynamics raise persistent questions regarding preparedness, responsibility, and governance. In his analysis of critical infrastructure systems, Brown (2006: 17) highlights persistent debates over what merits protection, the acceptable costs involved, and the allocation of responsibility between state, local, and private actors.

## 3.1 Critical Infrastructure from Past until Present

Critical Infrastructure can be reconstructed and taught alongside international security debates. The list of what falls under CI has changed as time progresses and technology expands (Newbill, 2019: 761). While the term itself did not exist, systems vital to a nation's functioning have always been in place, and therefore, history offers abundant examples of strategic attacks on CI. In Ancient Greece, Sparta seized the main source of grain imports for Athens to strategically starve the city (Brown, 2019: 14). During WW2 the *Casablanca Directive* laid out the strategic bombing of Germany's infrastructure system, interrupting the delivery of goods and pushing the nation's economy to collapse (Brown, 2019:14). These two examples demonstrate the strategic and vital nature of CI, that when attacked can impose disastrous consequences for the civil population. In total, the aftermath of WW2 unraveled the horrific consequences of war on civilians to the international community and sparked the creation of the four *Geneva Conventions* prohibiting the targeting and destruction of "objects indispensable to the survival of the civilian

population," (Article 54, Convention IV) such as transportation systems and agricultural areas (Newbill, 2019: 768). These civil systems have now been incorporated into what many nation-states view as CI today.

The Cold War Era viewed the protection of CI through a civil defense and military lens to ensure continuity in case of war or nuclear attack. In the 1980s and 90s, the rise of the internet, the invention of the World Wide Web, and its rapid commercialization unraveled new “perils of increasing interconnectedness” (Brown, 2019: 16). Suddenly, not only the physical infrastructure itself was vulnerable. Vital infrastructure systems (e.g. transportation, utilities, banking) came to be dependent on computers and with that they were vulnerable to organized crime and terrorism (Brown, 2019: 15). Within this changing landscape and due to major incidents like the *Oklahoma City* bombing in 1995 the U.S. took the leading role in formalizing the concept of CI in the 1990s (Brown, 2019: 9). The 1997 *Critical Foundations report* defined critical infrastructure as physical and cyber-based systems essential to national stability (Newbill, 2019: 761). The 9/11 terrorist attacks served as a major turning point, as they exposed the vulnerability of civil infrastructure to non-state actors. This led to a significant expansion of what was considered critical, now including health, finance and transportation sectors in the nation's protection strategies (Brown, 2019: 14). The European Union followed with its own framework in 2008 (European Commission, 2025).

From the 2010s onward, the protection of CI became increasingly dominated by cyber operations, hybrid threats, and geopolitical competition. In 2010, the *Stuxnet malware* demonstrated that cyberattacks could produce physical destruction of industrial control systems (Kaspersky, 2025). *Russia’s repeated intrusions into Ukraine’s power grid* in 2015 and 2016 marked the first known instances of cyberattacks intentionally shutting down electricity in a sovereign state (Newbill, 2019: 772). At the same time, ransomware emerged as a global threat with the 2017 *WannaCry and NotPetya attacks* disrupting hospitals, logistics networks, and shipping companies worldwide (Hern, 2017).

The 2020s further accelerated the trend toward systemic vulnerabilities. The *COVID-19 pandemic* exposed the fragility of health infrastructure, medical supply chains, and global logistics networks (Filip et al., 2022). Russia’s invasion of Ukraine in 2022 reinforced CI as a battlefield virtually and physically showing the hybrid nature of contemporary conflict i.e. missile strikes on energy grids, efforts to sabotage undersea cables and pipelines, cyber and drone operations, espionage, ransomware and much more (Edwards & Seidenstein, 2025: 3). More recently, the rapid expansion of AI systems, satellite constellation and cloud computing have led to their recognition as vital components to CI.

## 3.2 Current State and Relevance Today

### 3.2.1 Defining Critical Infrastructure

The last section depicted how critical Infrastructure has evolved alongside the evolution of today’s society. This raises the question of what should and can be defined as critical infrastructure. Shortly answered, there is no commonly accepted definition of critical infrastructure. Nevertheless, it is important to know what states perceive as CI to avoid misperception and escalation. Furthermore, countries that have codified their CI sectors have been more successful in establishing valuable measures to protect CI. However, views vary by member states of the UN, but tendencies and trends can be extracted when mapping the world's critical infrastructure sectors (Laumann et al., 2023: 2).

A study conducted by the German Council on Foreign Relations (Laumann et al., 2023) maps common CI sectors worldwide:

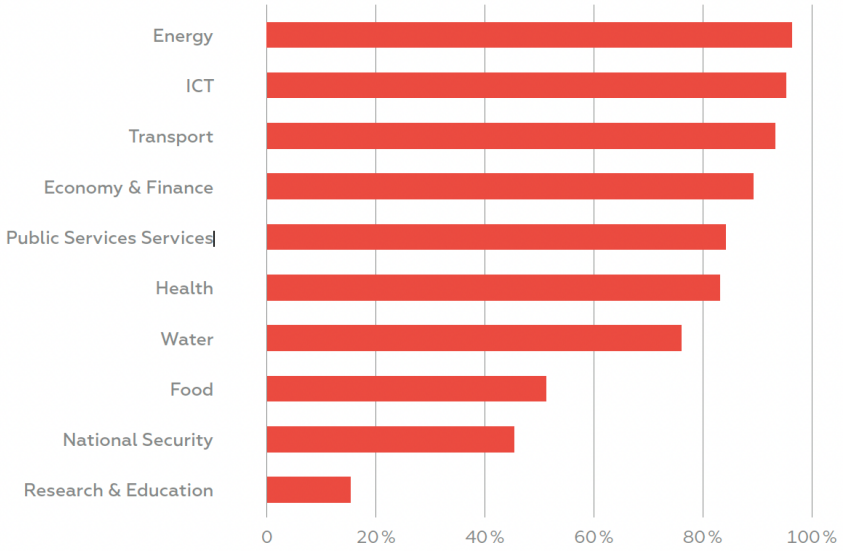


Figure 1 - Inclusion of specific sectors (in %) among the 100 countries that have published lists of CI sectors (2023: 5)

Figure 1 illustrates the extent to which specific sectors are included in national critical infrastructure (CI) sector lists, expressed as percentages across countries. It shows that the most frequently designated sectors are energy (96%), information and communications technology (ICT) (95%), transport (93%), economy and finance (89%), public services (84%), as well as health (83%). By contrast, sectors that are least commonly classified as critical infrastructure include research and education (15%), national security (45%), food (51%), and water (76%) (Laumann et al., 2023: 1). Thus, countries value CI sectors differently (Newbill, 2019: 764).

Furthermore, they find that priorities vary within regions (Figure 2):

| Regions | Europe | North America | Latin America & the Caribbean | Africa | Oceania & Australia | Asia | Global |
|---|---|---|---|---|---|---|---|
| Number of Countries | 44 | 2 | 33 | 54 | 14 | 47 | 194 |
| Number of Countries with lists of CI | 42 | 2 | 14 | 15 | 4 | 23 | 100 |
| Energy | 42 | 2 | 12 | 13 | 4 | 23 | 96 |
| ICT | 38 | 2 | 14 | 15 | 4 | 22 | 95 |
| Transport | 40 | 2 | 13 | 12 | 4 | 22 | 93 |
| Health | 36 | 2 | 12 | 12 | 2 | 19 | 83 |
| Food | 28 | 2 | 6 | 8 | 2 | 5 | 51 |
| Water | 33 | 2 | 10 | 11 | 3 | 17 | 76 |
| Public Services | 35 | 2 | 10 | 13 | 2 | 22 | 84 |
| Economy & Finance | 37 | 2 | 11 | 13 | 3 | 23 | 89 |
| Research & Education | 5 | 0 | 2 | 4 | 1 | 3 | 15 |
| National Security | 17 | 2 | 8 | 7 | 1 | 10 | 45 |

Figure 2 - Regions and their CI Sectors (DGAP, 2023: 7)

Regional specifications can be extracted from Figure 2. In general, among the countries with specified sectors, the category incorporated by nearly all is energy, followed by ICT and transport. Compared to other regions, Latin America stands out as the only place worldwide where energy only holds third position. However, environmental elements are seen as essential components of CI in this region. Brazil stands out by focusing on biosafety and bio-protection, reflecting a commitment to safeguarding biological resources. In North America (here: USA and Canada),

only research and education are not considered critical. In Europe, Russia includes “Russian legal entities and individual entrepreneurs who own information systems” and “Russian legal entities and/or individual entrepreneurs that ensure the interaction of these systems and networks” as critical sectors (2023: 6f.).

### 3.2.2 Structural inequalities

Many countries, particularly in Asia and Africa, face structural inequalities in the development and categorization of CI sectors, which significantly undermine their preparedness and resilience. While high-income countries have largely institutionalized CI identification and risk governance frameworks, many low- and middle-income states lack the administrative capacity, technical expertise, and financial resources necessary to do so. As a result, 94 countries in Asia and Africa still do not possess adequate national response or protection plans for critical infrastructure, leaving essential sectors such as energy, water, transport, and digital networks highly vulnerable to disruption (2023, 6f.). This disparity reflects broader global inequalities in state capacity and risk governance, where countries facing the highest exposure to climate change, political instability, and rapid urbanization are often the least equipped to manage systemic infrastructure risks (Hallegatte et al., 2019). Consequently, CI insecurity in these regions is not merely a technical deficit but a manifestation of global inequality, reinforcing uneven development and increasing dependence on external support.

### 3.2.3 The Private – Public Dilemma

The private–public dilemma in critical infrastructure protection (CIP) arises from the fact that most critical infrastructure is owned and operated by private actors, while the consequences of failures are borne by society as a whole. This creates structurally conflicting incentives: private operators prioritize cost efficiency and profitability, whereas governments focus on national security, public safety, and resilience. As a result, responsibilities for risk prevention, investment in security, and crisis response remain fragmented and often contested across governance levels (Brown, 2019: 18). Without clear regulatory frameworks and coordinated public–private partnerships, this misalignment undermines comprehensive CIP and leaves systemic vulnerabilities insufficiently addressed (OECD, 2019: 13f.)

### 3.2.4 Common threats:

CI faces a range of threats that can disrupt essential services and pose significant risks to public safety, national security, and economic stability. IBM provides a comprehensive list of common threats, including (IBM, 2025):

1. **Cyberattacks:** Attackers may target control systems, networks, and software vulnerabilities to gain unauthorized access, disrupt operations, steal sensitive information or cause physical damage.

2. **Physical attacks:** Sabotage, terrorism, or vandalism can directly damage facilities, disrupt operations, and endanger lives. These attacks can target commercial facilities, transportation systems, critical manufacturing operations, or other assets.

3. **Natural disasters:** Hurricanes, earthquakes, floods, wildfires, and severe weather events can disrupt essential services. Systems based on historical climate patterns may face challenges due to the increased frequency and intensity of extreme weather events.

4. **Pandemics and health emergencies:** Pandemics and disease outbreaks can cause workforce shortages, operational disruptions, and increased demand for healthcare services that can strain public health responders and overall system resilience.

5. **Supply chain vulnerabilities:** Vulnerabilities in the supply chain, such as compromised or counterfeit products, can introduce weaknesses that may be exploited to disrupt operations or compromise system integrity.

6. **Technological dependencies:** As critical infrastructure becomes more interconnected and reliant on advanced technologies, dependencies on complex systems and software increase.

### 3.2.5 Interconnectedness and Interdependencies of CI

Especially, the fact that globalization and the rise of information and communication technologies have led to global value chains has increased interconnectedness and interdependencies between vulnerable sectors and countries worldwide (OECD, 2019: 22). Figure 3 illustrates these new network interdependencies. Consequently, a failure or disruption of one CI system can have far-reaching consequences on other sectors and locations, sometimes globally. For instance, the large-scale floods in Bangkok in 2011 tremendously affected the car industry in Japan and its economy, as suppliers located in the flooded area were disrupted. CI is especially vulnerable to these shock events, such as flooding or natural hazards. Windstorms can make electricity transmission and distribution overhead lines fall down, earthquakes can break water pipes, destroy bridges or tunnels, floods and other water-related disasters can have large impacts on roads, railways, water supply and sanitation facilities, and storm surges and tsunami affect harbors, energy facilities and other infrastructure located in coastal areas (2019: 18). For further insights as well as policy recommendations, we recommend the *Good governance for critical infrastructure resilience*, OECD 2019 report.

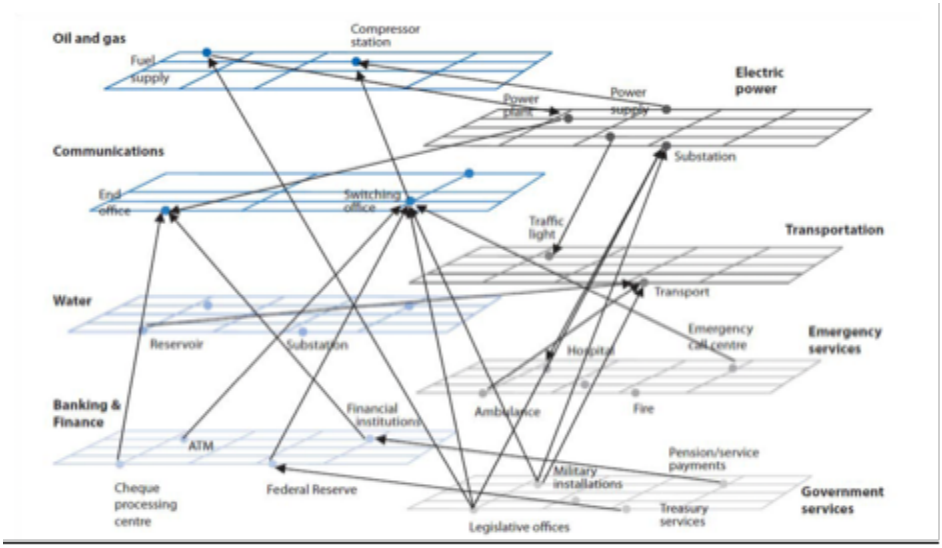


Figure 3 - Utility and network interdependencies (OECD, 2019: 22 extracted from NARUC The National Association of Regulatory Utility Commissioners, 2005)

-

# 4. UNSC and UN contributions to the issue; current legal framework

The United Nations have recognized the strategic importance of protecting critical infrastructure from state and non-state threats across several organs and specialized agencies. The protection of critical infrastructure was explicitly emphasized in Security Council Resolution 2341 (2017) as a relevant matter, warranting Council attention within the counter-terrorism context. This resolution affirms that attacks against infrastructure can have far-reaching effects on populations and economies and calls on Member States to strengthen protection measures and international cooperation. However, the UN contributes to the protection of critical infrastructure primarily through norm-setting, capacity-building, and technical guidance. Its role is not operational in the sense of defending infrastructure directly, but it builds frameworks, coordinates states, and strengthens resilience.

## 4.1 The protection of critical infrastructure by UN bodies and associated entities

UN specialized agencies steadily contribute technical expertise and capacity support. The *International Telecommunication Union* (ITU), for instance, maintains guidance, toolkits, and normative material aimed at strengthening national cyber resilience and protecting infrastructure supporting telecommunications and digital

services. The ITU's toolkits, guidance documents, and capacity building initiatives seek to harmonize technical standards and assist states in risk assessment, incident response, and resilience planning (ITU, 2025).

The *United Nations Institute for Disarmament Research* (UNIDIR) and other policy bodies perform an important bridging function between technical practice and diplomacy. UNIDIR's research outputs and convening examine threats to critical information infrastructure, promote conceptual tools for analyzing intrusion pathways, and support dialogues on cross-sectoral protection measures. Such work informs diplomats, policy-makers, and the Security Council by translating technical risk assessments into policy-relevant analysis. It thus enables complex technical and infrastructural issues to be made comprehensible and applicable for diplomats and politicians, particularly in the field of cyberspace security (UNIDIR, 2025).

The *United Nations Development Programme* (UNDP) advances cyber resilience and infrastructure protection from a development and capacity perspective. UNDP programming emphasizes the "people, protection, policy" pillars: strengthening human capacity and institutional frameworks, advising on protective measures for essential services, and fostering norms and regulatory regimes that reduce vulnerabilities. UNDP has also engaged in country programs and pilot projects, often in cooperation with ITU and hence using synergy effects, to develop national cyber strategies, incident response capabilities, and sectoral contingency plans (UNDP, 2022: 41ff.).

In addition, UN-associated institutions are strongly involved in capacity building for resilience against disruptions to critical infrastructure in a variety of sectors. Entities such as the *UN Office for Disaster Risk Reduction* (UNDRR), the *International Civil Aviation Organization* (ICAO), or the *World Bank* have created the necessary structures, provided detailed information material such as in-depth guidebooks, studies, and readers, and made financial assistance available in order to promote the protection of critical infrastructure in their respective areas of work (UNDRR, 2022; ICAO, 2022; World Bank, 2022).

## 4.2 The protection of critical infrastructure in UN lawmaking

The Security Council's practice reflects two principal tracks relevant for critical infrastructure. First, the Council addresses protection of infrastructure directly where attacks are linked to terrorism, as in Resolution 2341 (2017), which serves as a legal and political anchor for Council engagement on infrastructure protection in counter-terrorism settings. Second, critical infrastructure protection appears across counter-terrorism, sanctions, and peacekeeping mandates where the Council has required parties to protect civilian infrastructure or has directed peacekeepers and sanctions regimes to consider infrastructure security as part of broader stabilization objectives. These references indicate that the Council treats infrastructure protection as both a security imperative and a component of civilian protection and stabilization strategies.

Despite these developments, there remain governance gaps and coordination challenges. The regulatory and operational responsibilities for many critical systems are distributed across national ministries, private operators, and international bodies. The transnational nature of cyber threats in particular raises questions about attribution, jurisdiction, and the thresholds for collective responses under the UN Charter. Interagency coordination, public-private partnerships, and clearer operational doctrines for protecting cross-border infrastructure remain priorities for the international community and for any Security Council consideration of sustained responses (UNGA, 2021).

Practical policy guidance, therefore, emphasizes a mix of prevention, preparedness, and response. Prevention rests on resilience measures such as redundancy, network segmentation, and supply chain risk management; preparedness requires incident response plans, exercises, and information-sharing mechanisms; response requires legal frameworks for mutual legal assistance, norms for intergovernmental cooperation, and clarity on thresholds for invoking collective measures. The UN system's comparative advantage lies in convening states, shaping norms, and delivering capacity development, while specialized agencies and technical partners translate those norms into operational practice.

# 5. Case studies

## 5.1 The Panama Canal: Choke point, systemic exposure and risk vectors

The Panama Canal is a strategic maritime choke point that links the Atlantic and Pacific seaboards and thereby facilitates a substantial share of global maritime trade. Disruptions to its operation, whether from prolonged drought, physical damage, cyber intrusion, or deliberate sabotage, trigger immediate and cascading effects across shipping schedules, freight costs, and global supply chains. Analyses by UNCTAD and leading logistics consultancies have shown that restrictions on canal transits can reallocate millions of tonnes of cargo to longer routes, increase voyage times, and materially raise shipping costs for exporters and importers (UNCTAD, 2021).

The canal's vulnerabilities are multidimensional. Firstly, it is environmentally vulnerable: The canal's operation highly depends on freshwater reserves for lock operation, and drought conditions have, in recent years, forced transit restrictions that reduced vessel capacity and increased waiting times. Such climate-related exposure demonstrates that infrastructure vulnerability can be physical and environmental as well as humanly caused. In 2023 and 2024, drought episodes drew international attention to how climate variability and water management choices can sharply constrain a critical global artery (The Guardian, 2023).

A second class of vulnerabilities derives from the canal's concentrated topology and limited redundancy: As a narrow transit corridor handling a large volume of containerized cargo and bulk commodities, any prolonged stoppage or slowdown forces rerouting through longer passages such as Cape Horn or the Suez Canal. This creates bottlenecks in port capacity, warehousing, and inland logistics. Business strategy analysts estimate that substantial reductions in canal throughput can affect tens of millions of tonnes of cargo and prompt a structural reshaping of trade flows (McKinsey & Company, 2024).

Cyber and hybrid threats constitute a third vector. Ports and canal control systems increasingly rely on digital management systems for scheduling, vessel traffic services, tolling, and water resource management. A targeted cyber incident could degrade traffic management, falsify scheduling data, or impair the canal's operational control systems. In addition, denial-of-service attacks on logistic service providers or on payment and reservation systems can magnify operational paralysis even if physical locks remain intact. The intersection of cyber risk with legacy industrial control systems heightens the potential for disruptive cascades.

Subsequently, the Panama Canal illustrates the geopolitical and development dimensions of infrastructure vulnerability. The canal's smooth operation is not merely an economic concern for maritime firms; it is a matter of global economic stability for many developing and developed countries alike. Disruptions tend to hit economies with limited buffer capacity hardest. This case underlines that infrastructure protection requires cross-sectoral planning that spans water management, environmental policy, cyber resilience, and contingency operations.

## 5.2 Taiwan's semiconductor industry: strategic centrality and systemic fragility

Taiwan's semiconductor industry, and in particular the global role of leading fabrication companies, occupies a central and irreplaceable position within the modern digital economy. Semiconductors are foundational inputs across defense, telecommunications, transportation, medical devices, and consumer electronics. The concentration of advanced wafer fabrication capacity in Taiwan creates a systemic dependence: A major disruption there could produce shortages across multiple critical sectors worldwide. Policy reports and industry studies highlight that even temporary capacity constraints can cause long lead times and production losses for downstream manufacturers (US-Taiwan Business Council, 2023).

The industry's vulnerabilities take several forms. First, geopolitical risks: Taiwan's unique political status and cross-strait tensions present the prospect of state-level coercion or military intervention that could threaten production facilities or access to exports. Second, supply chain interdependence: Fabrication is only one step in a complex ecosystem that depends on specialized equipment, precursor chemicals, design tool chains, and logistics, much of

which is geographically dispersed but tightly synchronized. Third, cyber and insider threats: Semiconductor manufacturing relies on highly automated and data-driven production systems. Cybersecurity incidents, intellectual property theft, or targeted sabotage could interrupt node-level production and undermine trust in supply chains.

The industry's operational model also amplifies exposure. High capital intensity and the economies of scale associated with advanced nodes mean that capacity is concentrated in a limited set of ultra-advanced fabs. The production profile is such that scaling up elsewhere requires substantial lead time and investment. Consequently, resilience measures based purely on market substitution are weak in the short to medium term; strategic stockpiles, diversified sourcing, and cooperative industrial policy have therefore been proposed to buttress resilience.

Cybersecurity episodes in the semiconductor sector have demonstrated concrete risks. Public reporting has documented incidents that disrupted operations or exposed vulnerabilities in manufacturing-execution systems. These incidents have prompted industry practitioners and national authorities to intensify efforts to develop sectoral cybersecurity standards, cross-firm information sharing, and joint incident response protocols. The dual civilian and military applicability of advanced chips also raises unique national security considerations that intersect with trade policy and export controls (Feller: Manufacturing Dive, 2025).

### 5.3 Comparative implications for global security and policy lessons

Taken together, Nord Stream 2, the Panama Canal, and Taiwan examples underscore two complementary attributes of modern critical infrastructure: First, systemic centrality since certain nodes produce outsized global effects because of traffic concentration or unique capability. Second, multi-vector vulnerability as risks derive from environmental stress, physical sabotage, cyber disruption, and geopolitical tension, often acting in combination. For the Security Council, these attributes imply that protective measures require cross-domain analysis, international cooperation, and both immediate contingency planning and longer-term structural resilience measures.

Policy prescriptions that draw on these case studies emphasize diversification, redundancy, and cooperative governance. For maritime choke points, this includes investments in alternative routing, improved water governance, port resilience, and harmonized incident reporting. For sectoral concentration like semiconductors, this includes incentives for geographic diversification of production, shared standards for cybersecurity in industrial control systems, and export control regimes that are cognisant of supply chain effects. It also includes enhanced transparency among states about national stockpiles of critical components. Capacity building through UN agencies and regional organizations can reduce asymmetric vulnerabilities for smaller states.

At the operational level, the UN system can play a constructive role by facilitating norm development, providing convening and mediation services, and delivering capacity development. The Council's tools, resolutions, mandate language in peacekeeping operations, and references in counter-terrorism frameworks can help integrate protection of critical infrastructure into wider security planning. Yet the Council's action will remain most effective when paired with technical implementation by specialized agencies, robust public-private partnerships, and multilateral cooperation that recognizes the shared nature of many infrastructure systems.

## 6. Guiding questions:

- Which sectors does your country define as critical infrastructure, and how do national priorities and threat perceptions shape this definition?
- What are your country's key vulnerabilities regarding critical infrastructure?
- How should responsibility be allocated between state authorities, private infrastructure operators, and international organizations in the protection of critical infrastructure, especially given widespread private ownership?

- What constitutes critical infrastructure in the context of international peace and security, and is a minimum common understanding necessary for effective multilateral cooperation?

- How can the United Nations Security Council address transnational threats to critical infrastructure that occur below the threshold of armed conflict, particularly in cyberspace and hybrid warfare contexts?

# 7. Bibliography


Brown, K. A. (2006). *A brief history of critical infrastructure protection in the United States* (1st ed.) [Book]. Spectrum Publishing Group, Inc. http://cip.gmu.edu/wp-content/uploads/2013/07/CIPHS_CriticalPath.pdf

De Felice, F., Baffo, I., & Petrillo, A. (2022). Critical Infrastructures Overview: Past, Present and future. In Carlos Oliveira Cruz (Ed.), *Sustainability* (Vol. 14, p. 2233). MDPI. https://doi.org/10.3390/su14042233

Edwards, C., & Seidenstein, N. (2025). *The scale of Russian sabotage operations against Europe's critical infrastructure*. The International Institute for Strategic Studies. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf

Edwards, C., Seidenstein, N., & The International Institute for Strategic Studies. (2025). *The scale of Russian sabotage operations against Europe's critical infrastructure*. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf

European Commission. (2025, September). *Critical infrastructure resilience at EU-level*. Migration and Home Affairs. https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en

Filip, R., Puscaselu, R. G., Anchidin-Norocel, L., Dimian, M., & Savage, W. K. (2022). Global Challenges to Public Health Care Systems during the COVID-19 Pandemic: A Review of Pandemic Measures and Problems. *Journal of Personalized Medicine*, *12*(8), 1295. https://doi.org/10.3390/jpm12081295

Hallegatte, S., Rentschler, J., Rozenberg, J., & International Bank for Reconstruction and Development / The World Bank. (2019). LIFELINES. In *LIFELINES*. International Bank for Reconstruction and Development / The World Bank. https://doi.org/10.1596/978-1-4648-1430-3

Hern, A. (2017, December 30). WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017. *The Guardian*. https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

IBM. (2025, November 17). *Critical Infrastructure*. https://www.ibm.com/think/topics/critical-infrastructure

Laumann, E., Pericàs Riera, M., & Weber, V. (2023). Mapping the world's critical infrastructure sectors. In German Council on Foreign Relations, *POLICY BRIEF: Vol. No. 35*.

Newbill, C. M. (2019). Defining critical infrastructure for a global application. In *Indiana Journal of Global Legal Studies* (Vol. 26, Issue 2, p. Article 11). https://www.repository.law.indiana.edu/ijgls/vol26/iss2/11

OECD. (2019). *Good governance for critical infrastructure resilience*. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/04/good-governance-for-critical-infrastructure-resilience_7d5a9993/02f0e5a0-en.pdf

*Stuxnet Definition & Explanation*. (2025, October 6). /. https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet