DISEC

Study Guide

ENSURING THE
PROTECTION OF CRITICAL
INFRASTRUCTURE

Table of Content

1. Letter From the Secretary General

Most esteemed participants of FLZMUN’25,

I, as the Secretary General of FLZMUN’25, welcome you all to the first edition of this prestigious conference.
It is an honor and a pleasure to be able to present to you what we have been preparing for months and dreaming for years. My team has worked tirelessly to bring the best you have ever seen, starting with our organization to our academics.

Our objective is to facilitate proficient and elevated diplomatic deliberations, fostering valuable and constructive solutions throughout the duration of FLZMUN’25, enriched by the collective contributions of all participants. As a delegate, your journey begins here, with the study guide prepared by our dedicated members; your most honorable chairboard.

I advise you to read this study guide thoroughly and expand your research on different perspectives; focusing on your allocated country. It is essential to bear in mind that each nation and every perspective holds significance if you are adequately prepared to engage with the agenda at hand.

You have my best wishes for success and enriching discussions during these two days of enjoyment. I eagerly anticipate witnessing the valuable contributions you'll make to our conference.

Mehmet Onur ÇİĞDEM
Secretary-General of FLZMUN’25

2. Letter From the Under-Secretary General

Esteemed Participants of the ModernMUN'24 DISEC Committee,

I am delighted to be your guide and Chair in this conference and I wish you all a great experience. Our committee, DISEC, will put an emphasis on the topic of **Ensuring the Protection of Critical Infrastructure** and its components concerning modern conflict. Critical infrastructure is such a crucial part of our daily lives that if it were to fail, it would cause major problems in our interconnected global society. Our way of life is constantly under threat every day from cyberattacks, physical sabotage, hybrid warfare operations, and various forms of coordinated disruptions. The protection of critical infrastructure stands as the primary defender of our modern world, fighting a never-ending battle against these threats. Long story short, safeguarding critical infrastructure is our first and only line of defense against disruptions that can destabilize societies, harm civilians, and weaken national security. Many nations of the world employ different ways to protect such essential systems at their own discretion, whether through physical security, digital defense, early warning systems, or international cooperation. In many ways, the global infrastructure network is protected with sophisticated technology and methods. These methods can be strong and complex, but nothing is invincible. As you will witness in our guide, there are flaws to every system and anything can be vulnerable under the right conditions.

While reading this study guide, you will learn about historical instances where critical infrastructure has been targeted, how hybrid attacks and cyber-enabled terrorism are conducted and utilized in modern conflict, and the pivotal role infrastructure protection plays in our everyday lives. We will dive deep into these topics and find ways to combat these issues effectively and efficiently. I hope and wish you all a happy and fruitful conference, and please, if you have any questions about our committee, do not hesitate to reach out to me.

Best Regards,
Ali Demir Budak - alidemirbudak0@gmail.com
Under-Secretary General of DISEC

3. Introduction to DISEC

The Disarmament and International Security Committee (DISEC), known as the First Committee of the United Nations General Assembly, is the UN's main platform for discussing how the world can remain safe, stable, and peaceful. Its work focuses on understanding and responding to the challenges that threaten international security—ranging from the spread of weapons to the rise of new technologies that can be used in conflict. DISEC examines issues such as the control and reduction of conventional weapons, preventing the spread of nuclear, chemical, and biological weapons, and strengthening the global rules and agreements that help keep nations accountable. Beyond managing traditional security concerns, the committee also looks at modern and emerging risks, including cyber threats, illicit arms trafficking, regional tensions, and military developments in space.

Although DISEC does not have the power to enforce its decisions, its discussions and resolutions shape how countries approach peace and security. By encouraging transparency, cooperation, and trust among Member States, the committee helps prevent conflicts before they escalate. It provides a space where nations can voice concerns, share perspectives, and work together on solutions grounded in dialogue and international law. In doing so, DISEC plays an essential role in ensuring that the international community adapts to new risks while maintaining the core principle at the heart of the United Nations: that peace is best preserved through cooperation, understanding, and collective responsibility.

4. Introduction to the Agenda Item

Most of us honestly don't think about the machinery running our lives. We wake up, flick a switch, and assume the lights will come on. We turn a tap and trust clean water will flow. We take it as a given that the internet will connect us and the emergency room doors will slide open if we get hurt. For the most part, these are just invisible background noise until the moment they stop. And when that silence hits, it is terrifying. A blackout isn't an inconvenience; it freezes hospitals, paralyzes public transport, and isolates entire communities. It takes only a few hours of darkness to expose just how fragile our modern routines actually are.

The only real urgency today derives from how fast our world has changed. Systems that used to be simple, mechanical, and isolated are now intertwined in a vast, digital nervous system. Our power grids, banks, airports, and food supplies are all glued together by software and the internet. As it makes life incredibly convenient, that connectivity also creates a dangerous domino effect: a glitch or an attack in one corner of the world can now ripple across borders in seconds and cause chaos for millions.

The threats have evolved, too. We used to look for physical bombs or sabotage. Today, the threat is often a silent string of code. We see state-sponsored hackers targeting power grids to flex political muscle, or criminal gangs holding hospital data hostage for ransom. On top of these malicious acts, we're always fighting extreme weather events that batter infrastructure that was never built to withstand such frequent climate shocks. This has spawned a new era of "hybrid warfare", a messy mix of digital strikes, misinformation, and physical pressure that happens in the shadows. These attacks leave no fingerprints, and they blur the line between peace and war. Then there's the complicated question of ownership: Governments don't own everything anymore; private companies control vast chunks of our power and data. Which begs the question: Who is actually responsible for national security? When a private server farm goes down, is it a state problem? The world is still trying to figure out the rules of engagement here. We also have to talk about inequality because we are only as strong as our weakest link. In a connected world, a security gap in a developing nation isn't just their problem; it can blow back on global trade and communication. We cannot solve this in isolation. This is where the United Nations steps in, trying to guide a very difficult

conversation. Getting countries to agree on digital governance is incredibly hard-everybody has different interests and levels of trust-but forums like DISEC are vital simply because they keep us talking. At the end of the day, this isn't about wires, cables, or servers. It's about people. It's about making sure a grandmother can call for help, a city can feed its residents, and an economy doesn't collapse overnight. Protecting critical infrastructure is really about safeguarding the trust and safety that let us live our lives. It is a reminder that in a deeply connected world, we have to look past our borders to protect the shared foundation of our future.

5. Historical Overview

The most striking shifts of our era have to do with the digital and physical worlds fusing together. Until recently, cybersecurity and physical security were completely separate realms: One was the domain of IT specialists, the other of guards at the door. That separation is almost gone today.

Modern infrastructure systems-power plants, water networks, and industrial facilities-increasingly share these very same digital environments we use for both everyday communication and office work. The troubling reality here is that a single compromised computer at the corporate office can theoretically become a gateway to manipulate an entire city's power supply.

Yet at the same time, it has become nearly impossible to identify who is behind an attack. In traditional warfare, you knew with a high degree of certainty who you were fighting. In the cyber domain, threats come out of the dark. States can hide their activity behind hacker groups, or even masquerade as run-of-the-mill crooks in order to avoid blame. How, ask governments, do you defend against an adversary you cannot see?

National security is no longer confined to physical borders; it now involves the protection of invisible digital networks that keep modern society running.

5.1. Cyber Threats

Cyber threats became a serious issue long before most people realized how deeply the digital world could influence real-life systems. In the early days of the internet, attacks involved website page tampering or malware that caused inconvenience instead of genuine damage. As more and more essential services-energy grids, water distribution networks, transportation systems, banking platforms-commenced gradual shifts to digital control, attackers found far more impactful targets.

By the 2000s, cyber operations were already being conducted to gather intelligence and for political leverage. Hacking proved to be a vital source for governments to keep track of their competitors, pilfer technological information, and surreptitiously study the weaknesses of critical infrastructure. These operations took on a fundamentally different character in the late 2000s and early 2010s as it became clear that digital attacks could have physical effects. The Stuxnet attack against Iran confirmed this in 2010. Rather than exfiltrating data, the malware manipulated the control systems of Iranian nuclear centrifuges, destroying real equipment. From that point forward, states could no longer view cyber tools as harmless digital intrusions since they clearly had the capacity to function like conventional weapons.

As more infrastructure became internet-connected for greater efficiency and remote access, the potential points of entry proliferated. Cybercriminals targeted hospitals, local governments, and public services with ransomware, knowing such targets could not afford even short downtime. State-sponsored actors began probing pipelines, electrical grids, and industrial facilities, often without attempting an immediate attack but rather as part of a reconnaissance effort to identify vulnerabilities to take advantage of in a future conflict. Today, cyber threats are considered one of the most significant dangers facing national infrastructure. That is not only because the attacks happen frequently but also because they can strike without warning and escalate quickly, leaving governments with very little time to respond.

5.2. Terrorism and Physical Attacks

Long before cyber warfare became a central global concern, critical infrastructure had already been vulnerable to more traditional physical attacks. Infrastructure often represented an efficient means for terrorist groups to create widespread disruption with relatively limited resources. This could include striking transportation hubs, energy facilities, or crowded public areas to instill fear, cause economic damage, and even trigger political instability-all in line with the strategic aims of terrorism.

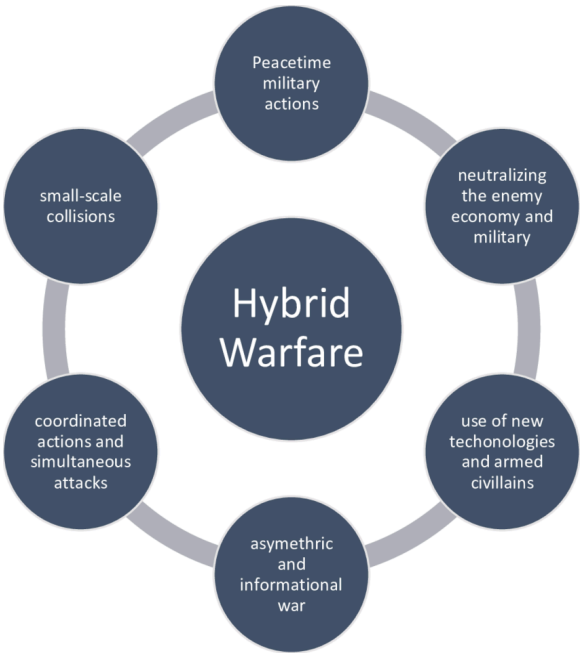
Attacks on public transit systems, oil installations, and governmental buildings throughout most of the late 20th and early 21st centuries have occurred in numerous countries. These actions make clear that infrastructure is symbolic and a practical target. Aside from national revenue, destruction to a pipeline suggests that a state is unable to protect its most precious assets. Other attacks, such as those against an airport or rail network, interrupt daily routines and leave indelible psychological marks on society.

Physical attacks on infrastructure continue to be a grave concern today. Still, hostile groups attempt to destroy electrical substations, communication towers, and even bomb places where many people congregate. What has changed is that most of these attacks now often blend physical with digital. Many modern operations are thus designed as combined assaults, with one form complementing the other. Cyber instruments could be used by a terrorist organization to shut off alarms, interfere with surveillance systems, or slow down emergency responses as a prelude to a physical strike. Consequently, the clear demarcation between digital and physical threats has largely vanished. The resulting fusion involves hybrid risks that are much more complex to foresee, detect, and defend against.

5.3. Hybrid Warfare and Emerging Technologies

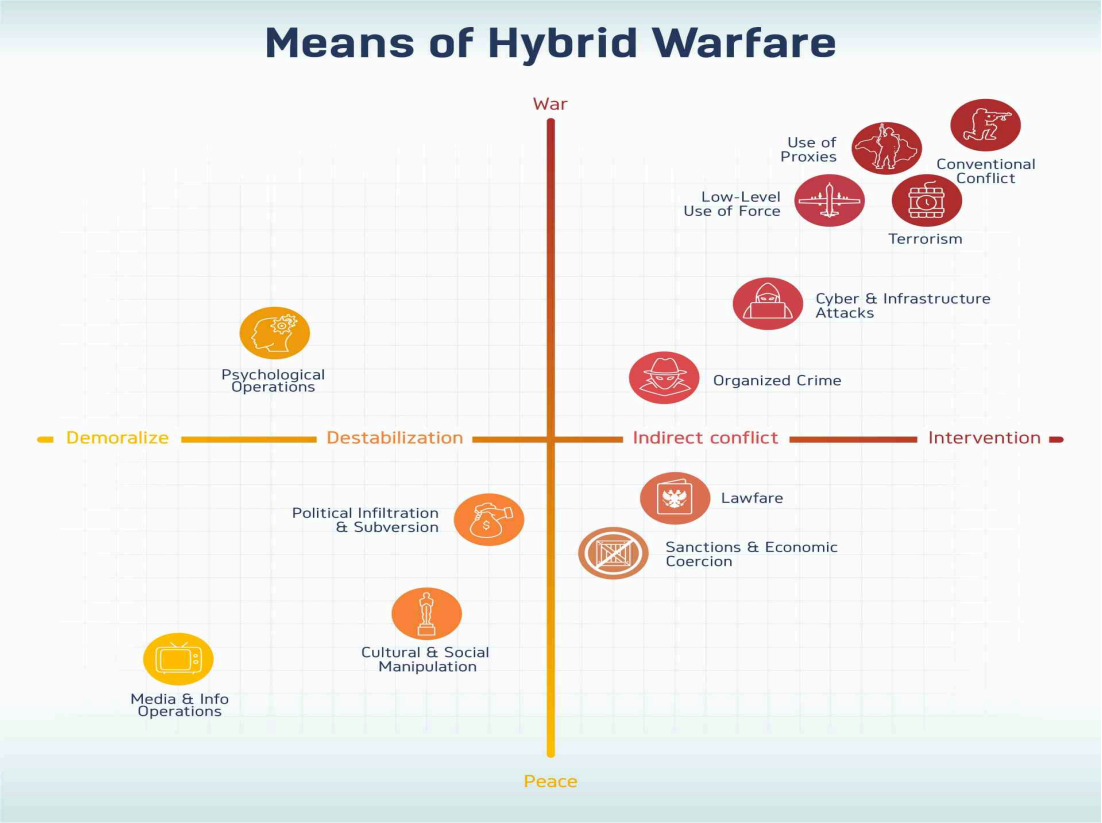
Hybrid warfare has become the newest and most complex stage in the evolution of threats against critical infrastructure. Rather than pursuing a single method, such as a fully cyber or fully physical attack, hybrid operations combine multiple techniques in innovative ways to be able to overwhelm the target. These campaigns may involve cyber intrusions, disinformation efforts, economic pressure, drone strikes, sabotage, or political interference, conducted either all at once or unfolding in a well-planned progression.

Hybrid tactics are attractive for two reasons: plausible deniability and disproportionate impact. A cyberattack that causes a section of a power grid to fail can easily be ascribed to criminal hackers, even when a government is responsible. Similarly, a drone strike on an oil facility, for which the expense is modest, can cause destruction comparable to a full-scale military attack. Disinformation provides another layer, as the dissemination of false or misleading narratives can weaken public trust when infrastructure failures occur, thereby making the government's crisis response far more complex.



Emerging technologies amplify these trends further. Drones that were once specialized military tools are now widely available and inexpensive, and many commercial models can be adapted for sabotage with minimal technical expertise. Artificial intelligence can rapidly identify system vulnerabilities or automate intrusion attempts at speeds no human observer could match. Meanwhile, the growing presence of Internet of Things devices-from smart meters to industrial sensors and automated controls-creates countless new entry points for attackers, since these smaller devices often rely on weaker security than the larger networks they connect to.

Hybrid war also transforms political and strategic thought. Infrastructure is no longer simply a technical asset in need of protection; it is now a theater of strategy in which states can exact pressure without escalating to open military conflict. The repeated attacks on Ukraine's energy grid, the operations targeting Saudi Aramco, and various pipeline disruptions around the world illustrate this reality. Taken together, these incidents illustrate how hybrid strategies can disable key services while maintaining sufficient ambiguity to avoid direct attribution and retaliation.



6. Understanding Critical Infrastructure

The term critical infrastructure tends to sound remote and technical, the province of policymakers or engineers, but what it actually refers to are the systems people depend upon every day, usually without any awareness of them. These systems form the bedrock of modern life, which enable predictable, stable functioning of society. We base our daily routines on the assumption, conscious or unconscious, that they will always work. When they do, they stay out of sight and out of one's mind. But when one of them stops working, even for one second, the consequences start to ripple right away, disrupting households, neighborhoods, businesses, and sometimes the whole national economy.

How important these systems are becomes clearer if we reflect on just how much society has changed in just a few decades. Until recently, many of these critical services operated in isolation from each other. Electricity grids were controlled by human regulators; water and sanitation systems relied on mechanical plants; airports depended on humans to choreograph takeoffs and landings; and hospitals kept patient records on paper. These older systems had their own vulnerabilities, but their limited interconnectivity meant that a failure in one component tended to remain localized. It could be a nuisance or dangerous, but it seldom had the potential for widespread disruption across a nation. Today, nearly everything is different. Most of the major systems in use today depend on some form of digital technology. Electricity grids interact with computerized controls that regulate supply and demand in real time. Airports depend on digital navigation systems, integrated security networks, and electronic scheduling programs. Hospitals maintain vast electronic files on patient histories, treatments, and diagnoses. Water treatment plants employ machines and sensors controlled by remote control that constantly monitor water quality. And the humblest utilities-traffic lights, heat, buses, metros-are controlled by their own silent digital web. All this sweeping connectivity carries enormous advantages: systems work faster and more efficiently, emergencies can be handled more effectively, and day-to-day life becomes easier. It follows that a problem in one place can spread quickly into others. A simple power outage can knock out communication systems, which in turn paralyze transportation and delay emergency services. Issues that hitherto would have been confined to their originating sector can jump into others in rapid succession, multiplying their impact while making recovery much more difficult. Because these systems are woven together under the surface of ordinary life, understanding what critical infrastructure really is, and just how deeply it constitutes everyday life, is crucial. It will explain why such systems are not solely a matter of technical expertise but form a core demand for national security, public health, and social stability. First, one must learn about their importance to appreciate why they must be safeguarded against natural disruptions and intentional attacks.

6.1. Categories of Critical Infrastructure

Although every nation defines critical infrastructure in its own way and adjusts priorities according to its local needs, the main categories remain strikingly similar across the world. This is because the basic requirements of modern societies do not differ very much. Energy almost always stands at the center of this framework, as no other system can function without it. Power plants, transmission lines, substations, oil and gas networks, and renewable energy facilities all work together to keep everything else running. When electricity fails, nearly every aspect of daily life comes to a halt: heating and cooling systems shut down, communications break, transportation slows, and essential services like banking and healthcare become severely disrupted.

Water systems hold an equally essential place in this structure. Clean drinking water, wastewater treatment plants, pipelines, reservoirs, and pumping stations are what enable communities to survive and maintain basic public health. A disruption in water availability or quality can escalate into a major crisis within hours, affecting millions of people and placing enormous strain on emergency services.

Healthcare infrastructure is another vital category that nations need to protect with much care. It includes hospitals, emergency medical services, pharmaceutical manufacturing and distribution, laboratory networks, and the digital systems where sensitive patient records are stored. Without a resilient healthcare system, even a relatively small incident-such as a localized disaster or a sudden outbreak-can quickly spiral into a national emergency.

Transportation infrastructure, including roads, rail lines, airports, seaports, bridges, and public transit systems, forms a country's economic circulatory system. Goods cannot be delivered, supply chains cannot operate, workers cannot get to work, and industries cannot function when transportation systems fail. Modern economies are especially dependent on vast logistics networks that cross entire continents; the stability of the transportation infrastructure is absolutely indispensable.

Communication and digital infrastructure have now become just as crucial as conventional utilities, such as electricity and water. Internet services, mobile networks, fiber-optic cables,

satellites, data centers, and cloud platforms all compose the nervous system of modern-day society. Governments, businesses, and people use digital communication to function. Even short periods of disruption will lead to huge economic losses and paralyze key services. Financial infrastructure forms another pillar of national stability. Banks, stock exchanges, credit systems, digital payment processors, and insurance networks undergird nearly every other sector. Modern economies rely on efficient and secure financial transactions. When these systems fail or are compromised, the consequences are both instantaneous and widespread.

Sectors such as food production and distribution, agricultural supply chains, waste management, and government administrative services-all vital to society and not always appearing at the front of every citizen's mind-clearly fit within the definition of critical infrastructure. As soon as any one of these sectors breaks down, society starts to destabilize. What might unite all these categories is their role in enabling daily life. These systems are not optional conveniences but fundamental necessities. Without them, modern society simply cannot function.

6.2. Why Critical Infrastructure is Vulnerable

The fact is, modern critical infrastructure is more vulnerable today than it has ever been, and the source of this vulnerability comes through a combination of long-standing weaknesses and new, rapidly evolving risks. Digitalization drives insecurity primarily. Many essential systems were never designed to be internet-connected; they were constructed decades ago with minimal security or designed under the assumption that they would remain isolated. When those systems were finally brought online to improve efficiency or reduce costs, they absorbed risks their original designs were never meant to accommodate. Thus, systems that once required physical access to compromise can now be breached through something as simple as a weak password, an outdated device, or a software vulnerability that was never patched. A similar concern is the age of physical infrastructure. For most countries, their power grids, pipelines, bridges, and transport networks are older than generally assumed. Such structures inevitably need maintenance at all times; when not invested in continuously,

they deteriorate gradually. Oftentimes, just one failure or even a surprise external shock can serve as a catalyst toward greater disruptions. When digital weaknesses are layered onto aging physical systems, overall risk goes up exponentially. The sophistication of cyber threats is also much more advanced than it used to be. The low-level, opportunistic hacking has, in many cases, transformed into a number of highly organized operations by professional groups, criminal networks, and even state-sponsored teams. An attacker might operate in hiding inside a system for months, first carefully studying its susceptibilities before orchestrating an attack. They may also target the industrial control systems that regulate physical processes, so a successful cyber attack might have real, tangible damage: power stations shut down, chemical balances in water systems altered, and emergency communication channels disrupted or fully disabled.

All these vulnerabilities are exacerbated by the increasing geopolitical tensions. Power grids, pipelines, data centers, and even structures of communication networks have turned, or are increasingly perceived as, strategic targets for adversaries. Critical infrastructure has silently become one more battleground of international competition. Hybrid operations-that mix cyberattacks, sabotage, disinformation campaigns, and economic pressure-enable states to cause harm while retaining plausible deniability and avoiding overt military conflict. The central role of the private sector introduces additional complexity. Governments rely on privately owned systems for everything from energy and telecommunications to finance and healthcare. There is an inherent tension between national security objectives and corporate imperatives. Governments care about resiliency and citizen safety; firms care about efficiency and profit. These disparate incentives will often produce shortfalls in security to be exploited by the attacker. Environmental stresses increasingly compromise infrastructure stability, too. This is partly due to climate change, which brings more destructive storms, floods, wildfires, and heat waves. These can hit all at the same time in a number of systems, overwhelming emergency responders and exposing structural weaknesses in infrastructure that was never meant to bear such extreme conditions. Human fallibility is an inevitable and too-often-underestimated point of failure. Infrastructure ultimately depends on human operators, and people make mistakes. One setting configured poorly, a worker being duped into clicking on a phishing email, or a late maintenance process opens entire networks to serious danger. The human factor in all this makes security not only a technical problem but also a behavioral issue. Taken together, the vulnerabilities mentioned here show that critical infrastructure protection is far more than an engineering issue. It is a national and

international priority covering technology, politics, economics, environmental change, and human behavior. These weaknesses can be addressed effectively only by cooperation across all of these areas.

7. Current Global Challenges

The task of protecting critical infrastructure has grown more complex than it has ever been before. Threats that were limited and predictable a number of years ago have now expanded into a wide range of interconnected risks. These dangers cross borders, affect multiple sectors at once, and blur the traditional boundaries of conflict. People expect modern infrastructure to be fast, efficient, and digitally enabled, yet these very expectations make the systems increasingly challenging to defend.

Today, governments are presented with risks that increase in speed beyond the pace of regulations, whereas technology changes at a rate much quicker than anything the global community could dynamically adjust to. Consequently, every nation is positioned at a precarious juncture where cyber dangers, political influences, economic flaws, and heavy dependence on the private sector are happening all at once. Critical infrastructure protection no longer pertains to the isolated attacker or to patching a particular vulnerability but has become an ongoing battle against a global backdrop characterized by instability and ambiguity.

The issues highlighted below are the most pressing problems facing any country which is compelled to address them.

7.1. State-Sponsored Cyber Operations

The most significant modern-day threat comes from nation-states that incorporate cyber capabilities into their grand geopolitical strategies. Operations are usually very structured and well-funded, with trained teams that can infiltrate highly sophisticated and well-defended systems. Unlike opportunistic cybercriminals, who are most often motivated by financial profit, state-backed actors respond to political motivations. Their goals can include weakening a foe, collecting sensitive intelligence, uncovering hidden vulnerabilities, or implementing strategic pressure without crossing the threshold for overt military action.

What makes these state-sponsored campaigns especially alarming is their quiet, long-term nature. These actors seldom attack immediately after gaining access but rather get a foothold inside networks and try to remain as unobtrusive as possible. Sometimes, it is months or years before anything can be detected. During that time, they learn how the system works, map out its weak points, and plant backdoors or dormant tools which enable them to return at will. Quite often, their presence is unsuspected until they act or until a large crisis of some sort forces further investigation. Another big challenge is the problem of attribution-who is really responsible. Even when a government thinks that it knows which state is responsible, proving it beyond all doubt is exceptionally difficult. Cyber operations may route through several countries, disguise themselves as ordinary criminal activity, or be deliberately engineered to resemble the modus operandi of another group. The uncertainty reinforces diplomatic tension. Some governments hold back because they are worried about blaming the wrong actor, while others retaliate against the wrong target and risk escalating conflict. State-sponsored cyber activity also plays a central role in hybrid warfare. Instead of physically destroying critical infrastructure, for instance, some governments go after the systems that undergird it-be it through the communication networks, through government databases, or through large supply chains. Others combine cyber intrusions with disinformation campaigns to create confusion at the precise moment a system fails. This blend of indirect pressure and intentional ambiguity has transformed state-sponsored cyber operations into strong instruments of influence and coercion-even when physical destruction does not occur.

7.2. Insider Threats

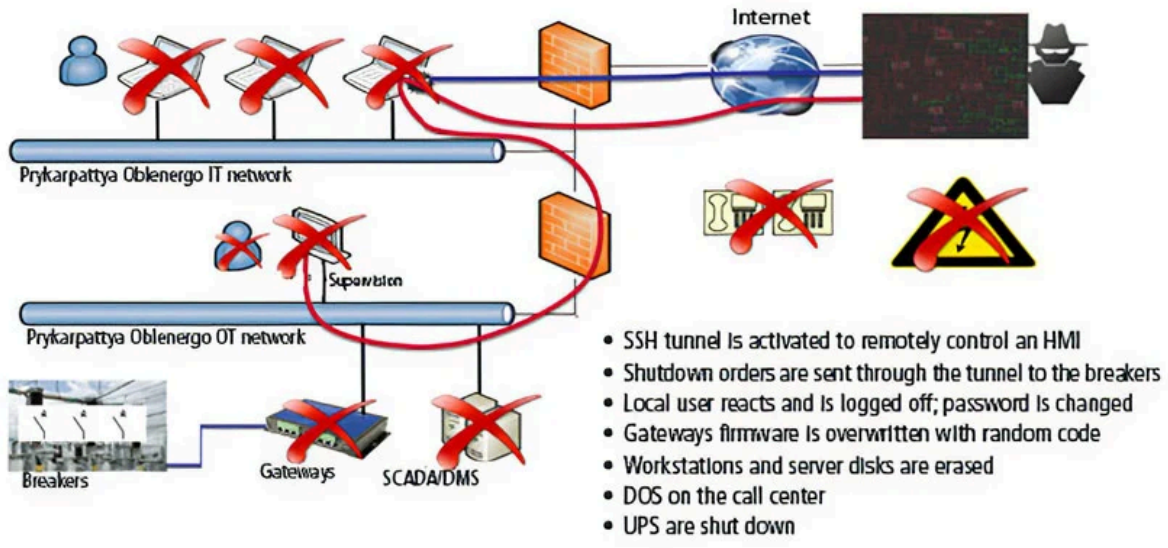
While highly publicized outside attacks tend to dominate headlines, some of the most dangerous threats to critical infrastructure actually come from within. Individuals with legitimate access to sensitive systems can cause enormous damage, sometimes intentionally and sometimes never meaning to. The insider threat can come from frustrated employees, contractors who work closely with the system, or individuals persuaded or manipulated by outsiders. Unintentional insider mistakes happen far more often than most people recognize. A tired employee might click on a phishing link without thinking, mis-configure a server during a busy shift or ignore a small security warning because it seems unimportant at the time. Yet even one small slip can open the door to attackers.

Since many infrastructure networks combine decades-old equipment with modern digital tools, a single mistake can create weaknesses that are surprisingly easy to take advantage of by adversaries. Deliberate insider threats are even harder to deal with. A person who knows internal details about a system can bypass almost any protection that would block an outsider. He or she could steal sensitive data, disable alarms, change software settings, or quietly allow unauthorized access into the system.

People act for all sorts of reasons: anger against an employer, financial benefits, coercion, or even ideological beliefs. Whatever the motive, the extent of damage an insider can achieve is often way beyond what an attacker from outside could ever manage singly. This is a problem operators of critical infrastructure constantly face: they must have sufficient staff to operate complex systems and that staff must be provided with access to critical tools and information; at the same time, every individual that has such access represents a potential threat. Background checks, surveillance systems, and more restrictive access controls may make that risk manageable but cannot eliminate it entirely. This makes the human factor arguably one of the least predictable and most daunting components of system security.

8. Case Studies

The true nature of critical infrastructure protection becomes clear once we examine real-life examples. Over the last two decades, a series of important events has shown just how vulnerable modern systems can be and how quickly one single disruption can escalate into a national crisis or even an international one. These incidents prove that attacks on infrastructure are not theoretical possibilities but real events that have played a defining role in global security debates.



Each case involves a different dimension of the evolving threat landscape. Some reveal how a cyber attack can bring essential services to a grinding halt in minutes. Others show hybrid operations where digital intrusions, coupled with physical sabotage, are used to amplify an impact. There are incidents where covert interference heightened geopolitical tensions and examples in which simple tools caused enormous economic damage. By researching these events, important insights are gained into how attackers operate, why systems fail, and how governments react when their infrastructure comes under strain. Such perspective is important in understanding why the protection of critical infrastructure became such an urgent, unavoidable priority in today's world.

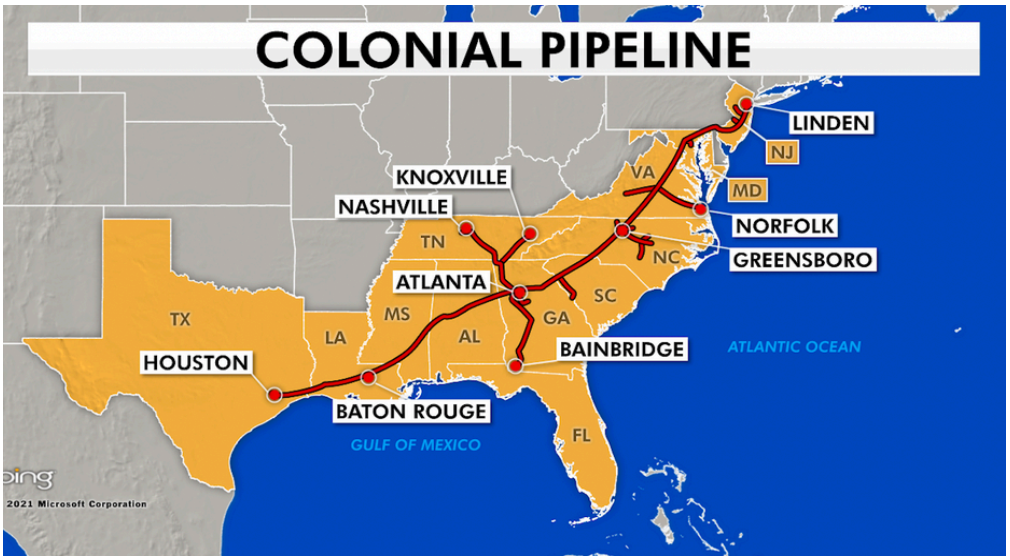
8.1. Ukrainian Energy Grid Attacks *(2015-2022)*

Ukraine is perhaps the clearest and most compelling example of how attacks on critical infrastructure can be weaponized in cyberspace. For over a decade, Ukraine has suffered from repeated and highly coordinated attacks against its essential systems. One of the first major incidents occurred in December 2015 when a well-planned cyber operation deliberately shut off parts of the national power grid. Using social engineering tactics, hackers gained access to the control systems operated by three regional electricity companies, remotely initiated the manual opening of circuit breakers, and left more than 200,000 people without electricity. What made this attack particularly daunting was that it was not just a digital disruption; it was a physical event with immediate, tangible ramifications. Operators watched in a state of helplessness as their systems were hijacked in real time, fully aware that they had neither control nor any ability to stop the unfolding crisis. A year later came another, far more complex attack-the Industroyer incident-which struck Kyiv's power grid and plunged parts of the capital into darkness for several hours. The malware used in this operation communicated specifically with industrial control systems-a capability which had previously been thought beyond all but the most advanced and best-resourced adversaries. It marked a pivotal moment in showing that cyber operations were evolving from espionage tools into weapons capable of causing large-scale physical harm.

This trend dramatically worsened in 2022, when the broader conflict intensified. Waves of cyberattacks paralleled kinetic military actions, striking at communications networks, government databases, satellite infrastructure, and energy systems. The fact that digital intrusions were deliberately synchronized with physical strikes provided an unusually vivid example of hybrid warfare in practice. The Ukrainian experience is telling not just because of the sheer number and regularity of the attacks, but also because it shattered long-held assumptions about the robustness of power grids. Systems believed to be solid and impervious were found to be vulnerable to remote digital manipulation. These events forced governments worldwide to reconsider their own levels of preparedness and to realize that their infrastructure may be far more exposed than had been assumed.

8.2. Colonial Pipeline Attack *(2021)*

The Colonial Pipeline Company is the operator of the largest fuel pipeline system within the United States, which came under a ransomware attack in May 2021. In record time, this led to widespread fuel shortages down the East Coast. In this instance, the attackers had not touched the pipeline's physical systems at all, but the company shut down operations as a precaution because there was concern that the malware could spread into critical components. This caused panic buying, long lines at gas stations, and temporary increases in fuel prices in several states.



The Colonial Pipeline incident was particularly noteworthy because it demonstrated just how vulnerable key supply chains can be. A single digital intrusion affecting the business side of a company, rather than its operational technology, was enough to disrupt a large portion of the nation’s fuel distribution. The attack prompted a substantial policy response from the United States government, including new cybersecurity guidelines for pipeline operators and enhanced cooperation between federal agencies and private companies. And it initiated important discussions about the requirements for national standards to protect critical infrastructure from ransomware.

The event made clear an uncomfortable reality: Critical infrastructure systems today are so interconnected that even a disturbance on the administrative or commercial side can quickly spiral out of control into a major operational crisis. It also showed that criminal groups-not just state actors-have the capability to create national-level disruptions using tools that are inexpensive, widely available, and increasingly simple to deploy.

8.3. Stuxnet *(2010)*

The Stuxnet attack has been referred to as one of the most defining cases of a cyber operation against physical infrastructure. First identified in 2010, Stuxnet was an extraordinarily sophisticated piece of malware engineered to infiltrate the Iranian nuclear program. It spread stealthily via infected USB drives and vulnerable network systems until it reached the centrifuges at the Natanz enrichment facility.

Once inside, Stuxnet manipulated the centrifuges' control systems to make the machinery rotate at speeds that would cause damage; meanwhile, it showed normal readings to operators. This deception let the malware quietly destroy about one thousand centrifuges without immediately raising alarms. This was a new attack on the world stage: a cyberattack designed to create specific, physical destruction of high-value industrial machinery.

What truly set Stuxnet apart, however, was not just its technical complexity but also the strategic message it conveyed: it showed that cyber tools could serve as a mighty weapon that might delay or damage a nation's key programs without resort to traditional military force. Since Stuxnet, governments all over the world have begun investing dramatically more in both cyber defense and offensive cyber capabilities. The incident fundamentally changed how states understand infrastructure security and the role that cyber operations can play in international conflict.

8.4. Saudi Aramco Abqaiq-Khurais Attack *(2019)*

The September 2019 attack on Saudi Arabia ranked among the most consequential strikes on energy infrastructure the world had seen in years. A coordinated drone and precision munitions assault on two major Aramco facilities-Abqaiq and Khurais-both considered linchpins in the global energy system due to their processing of a significant share of the country's crude oil-forced operations to grind to a halt. Suddenly, roughly five percent of the world's oil supply was removed from the market, with global prices surging almost immediately. The shock to the international energy markets was both swift and severe.

What made the attack particularly striking was how it revealed the vulnerability even of sites that are most heavily protected and of strategic importance. Despite layers of advanced security, these facilities proved susceptible to relatively inexpensive and widely accessible technologies such as drones. The attack also underlined the heavy extent to which global markets rely on a small number of key infrastructure points functioning as bottlenecks in the global energy supply chain. While Saudi Arabia restored production faster than many thought it would, the event sparked serious debate about the long-term security and resilience of oil infrastructure across the Middle East.

Beyond the economic consequences, the attack underscored the increasing challenge of attribution in modern conflict. A variety of groups and states were suspected, but nailing a definitive, publicly accepted conclusion proved remarkably hard. This ambiguity reflected a larger problem in contemporary security: even as emerging technologies make it easier to pull off complex attacks, they make it harder for the international community to determine who is responsible. Coordinated responses thus become more difficult, and global tensions can increase even when the perpetrator remains unknown.

8.5. Nordstream Pipeline Explosion *(2022)*

The apparent explosions that damaged both the Nord Stream 1 and Nord Stream 2 natural gas pipelines in September of 2022 represented one of the most politically sensitive infrastructure incidents to have occurred in living memory. The pipelines lie beneath the Baltic Sea and were much more than sections of energy infrastructure; they formed major strategic assets that played a central role in the greater European energy landscape. Tearing through the pipes, these blasts caused enormous gas leaks and ruptured a great deal of pipe length, rendering large parts effectively unusable. Pictures of bubbling gas rising to the sea surface turned into a powerful symbol of the vulnerability of even the most remote systems.

What happened subsequently did little to dissipate that sense of foreboding. To this day, the question of who was responsible is still debated. Different governments and spy agencies have floated competing theories, but none has reached that type of definitive, widely accepted conclusion necessary to settle the matter. The ambiguity fed geopolitical tension, contributing to mistrust among states and raising thorny questions about responsibility, deterrence, and intent. The uncertainty also drew global attention to the more general vulnerability of undersea infrastructure, including pipelines, fiber-optic cables, and the communication lines forming the invisible backbone of international connectivity.

Ultimately, the Nord Stream incident made crystal clear that sabotage of critical infrastructure can achieve a number of objectives simultaneously: geopolitical pressure, economic disruption, erosion of public trust, and signaling strategic intent-all without resort to overt

conflict. If anything, the event showed that even deep-sea infrastructures, which had been assumed to be safe due to their positions, are not that safe from covert operations. Many nations have thus been compelled to reconsider how they monitor, defend, and maintain underwater assets. Governments are increasingly realizing that such hidden systems are no less critical than those on land and that their protection must lie at the heart of modern infrastructure security strategies.

9. Questions to be Answered

1. What measures can states take to reduce the impact of hybrid warfare on critical infrastructure?

2. How should the international community define "critical infrastructure" in a way that supports cooperation without ignoring national differences?

3. Should cyberattacks on critical infrastructure be considered armed attacks under international law? If so, to what extent?

4. What responsibility do private companies hold in securing infrastructure that is essential to national security?

5. How can states balance security requirements with the need for innovation, connectivity, and technological openness?

6. What mechanisms should exist to support countries with limited resources or technical capabilities in protecting their infrastructure?

7. Should the UN or another international body establish minimum global standards for cybersecurity in critical sectors?

8. How can states cooperate and share information without jeopardizing national sovereignty or sensitive intelligence?

9. What should be the appropriate response when the perpetrator of a cyber or physical attack cannot be reliably identified?

10. How can governments address insider threats without creating excessive surveillance or limiting civil liberties?

11. How can infrastructure be modernized to withstand both digital and physical threats without causing disproportionate financial burdens?

12. What ethical considerations arise when enhancing surveillance or monitoring systems to protect infrastructure?

13. How can public awareness and preparedness be improved to reduce panic during infrastructure failures or attacks?

14. How should states approach future threats, such as AI-driven attacks, drone swarms, or quantum-based cyber intrusions?

10. Further Reading

For delegates who wish to explore the topic further, the following sources provide clear, reliable, and accessible information on critical infrastructure protection, cyber threats, and hybrid warfare:

UN Office for Disarmament Affairs – Cybersecurity and Disarmament
https://unoda.org/cybersecurity

NATO – Hybrid Warfare and Emerging Threats Overview
https://www.nato.int/cps/en/natohq/topics_156338.htm

CISA – Critical Infrastructure Sectors Explained
https://www.cisa.gov/critical-infrastructure-sectors

EU Agency for Cybersecurity (ENISA) – Threat Landscape Reports
https://www.enisa.europa.eu/topics/cyber-threats

World Economic Forum – Global Risks Report
https://www.weforum.org/reports/global-risks-report-2024

Council on Foreign Relations – Cyber Operations Tracker
https://www.cfr.org/cyber-operations/

11. Bibliography

CISA. (2023). Critical infrastructure sectors. *Cybersecurity & Infrastructure Security Agency.* https://www.cisa.gov/critical-infrastructure-sectors

Council on Foreign Relations. (2024). *Cyber operations tracker.* https://www.cfr.org/cyber-operations/

European Union Agency for Cybersecurity. (2023). *ENISA threat landscape.* https://www.enisa.europa.eu/topics/cyber-threats

Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. Doubleday.

Healey, J. (Ed.). (2013). *A fierce domain: Conflict in cyberspace, 1986 to 2012*. Cyber Conflict Studies Association.

Lindsay, J. R. (2015). *The impact of China on cybersecurity: Fiction and friction. International Security*, 39(2), 7–47. https://doi.org/10.1162/ISEC_a_00197

NATO. (2023). *Hybrid threats and hybrid warfare.* North Atlantic Treaty Organization. https://www.nato.int/cps/en/natohq/topics_156338.htm

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare.* Farrar, Straus and Giroux.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know.* Oxford University Press.

United Nations Office for Disarmament Affairs. (2023). *Cybersecurity and disarmament.* https://unoda.org/cybersecurity

United Nations Office of Counter-Terrorism. (2022). *Protecting critical infrastructure from terrorist attacks.* https://www.un.org/counterterrorism

Weiss, M., & Vyas, K. (2020). *Industrial cybersecurity: Case studies and best practices.* Wiley.

World Economic Forum. (2024). *Global risks report 2024.* https://www.weforum.org/reports/global-risks-report-2024

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon.* Crown.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2023). *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı.* https://www.cbddo.gov.tr

Erdin, M. (2022). *Kritik altyapıların siber güvenliği üzerine değerlendirmeler.* TRT Akademi Dergisi, 7(2), 34–52. https://www.trtakademi.net

Milli İstihbarat Teşkilatı. (2023). *Siber tehditler ve ulusal güvenlik cevrimici yayını.* MİT Başkanlığı. https://www.mit.gov.tr