NMMUN'25

BACKGROUND GUIDE

FIFA

CONTENTS

Letter from the chairs

It’s late at night, for the people of the working class it’s just a normal day, some are trying to work their way through a horrendous workload, while others are catching up on much-deserved sleep. The clock is ticking as it’s supposed to, the moon shines in its own glory, the world is as it’s supposed to be, untouched, just another peaceful night. But was it really peaceful? Was it the way it’s supposed to be? Was it the way everyone imagined it to be? Questions just flow through one’s mind as they sleep. Most people might be sleeping, but there are people who bring up those late-night conversations, those theories that a curious mind must have. Everything just flows through. A mind is curious, but what all could it do? Merely just have thoughts, right? Merely just a few fragments of a wide imagination. But does one ever realize that nightmares might not come true, but there is no reason in the world to defy their reality? People thought today was just a regular day but... are they right?

Simon, a mere 16-year-old, scrolls through Instagram as done by a normal kid his age at 2 in the night. Richard, an IT officer, goes through his files for his next presentation. Hannah goes through her notes for the upcoming exams on her computer. For state-controlled armies, it’s regulations as usual. But... they don’t know what’s about to hit them. What people thought would be a normal day turned into disaster — something one could only imagine in their wildest of nightmares. It’s 2:12.

Bank servers? Infiltrated. Computers? Shut. Lights? All blank. Servers? Crashed. Stock exchanges? Down to ashes as if they never existed.

The once known perfect globe called Earth went from shiny lights to a dark gloomy ball with life in it. The world is at risk, nothing seems to be working, every single operation controlled and maintained by state and national governments comes to a halt. The people start questioning why and what is going on while the leaders of each country start pointing fingers. No one knows what this is — was it an attack? Or was it just a mass power failure by accident? Questions are left to be answered, and you — delegates — are in charge of answering them. The world might have restored its power, but no one knows why and how it happened... or if it’s going to happen again.

Sounds a little intense? But it's interesting, it hooks one to its core. This might just be a simulation, but this is an issue that the world might face at any point in time. Welcome delegates to the Federal Communications Crisis Council — might sound complicated, but in simple terms, the world is at risk and it's up to you to solve this mystery. Crisis councils might sound a little scary at first, but we assure you it's an experience you won't forget.

And by we, I mean us — the chairs. Greetings delegates! We are Sreyas & Rachael, the Chairpersons of the FCC for NMMUN'25, and we are honoured to have you with us! Throughout the next few weeks, we will gather to solve this unknown entity. An MUN might be a little nerve-wracking, but we, the chairs, will make sure that each and every delegate has the experience of their lifetime. And if you ever think you're alone in this, remember that you aren't. It's okay to think that way, but all of us are here to reach one solution.

The two days of the conference will strike your nerves like nothing has before. Here, you aren't only being tested on your debating skills — it's your thinking that matters. It's how you deal with a sudden emergency. We, as the chairs, have only one piece of advice: research well, and remember... be wise — the world's safety is in your hands.

Rachael John
Sreyas Sreevalsan

Chairpersons, FCC

OPERATION BLACK VEIL

At 02:13 GMT, the world blinked. In Mumbai, commuters slept through the silence, unaware that their trains had stalled in place. Berlin's final S-Bahn cars rattled to a halt underground. In Boston, traders stared at dashboards that promised business as usual. In truth, the nervous system of modern civilization had failed.

Clocks froze. Air-traffic controllers lost all audio. Satellites rotated out of alignment, cutting their gaze from Earth. Undersea cables carried nothing but static. Power grids convulsed. The world's financial arteries clotted. And in that single, carefully engineered window of chaos, 4.1 billion dollars vanished into untraceable accounts. It was the largest theft in human history executed under the cover of a blackout no one saw coming. The transfer passed through shell accounts, anonymous wallets, and a Delaware crypto clearinghouse with a retired U.S. Navy admiral on its board. In India, the first signs appeared. Commuter trains stood motionless, the Reserve Bank's systems stuttered, and emergency channels went dark. National investigators at CERT-IN discovered that the blackout scripts had hijacked a NATO frequency to suppress Indian Rail's backup systems. Stranger still, the Reserve Bank's missing funds had been verified using a cryptographic quorum key, one that should only be accessible to regulators in the West. Yet system logs indicated the quorum had been reached in Dubai. To New Delhi, this no longer looked like a foreign incursion. It looked like betrayal from within the very Council meant to defend them.

Berlin woke to its own crisis. S-Bahn networks froze, Brandenburg's runway lights failed, and European internet exchanges faltered. Once again, the dashboards monitoring them reported nothing unusual. Forensics revealed that firmware had been seeded into satellites weeks before, smuggled in through routine update chains. At the center of those chains stood a Luxembourg contractor with undisclosed contracts to the NSA.

Moscow moved quickly. The Russian Ministry of Defense released packet traces they claimed to have captured in Berlin, showing exploits almost identical to EternalPatriot — an NSA cyberweapon exposed years earlier by the Shadow Brokers. Russian media repeated the accusation relentlessly: WHY,

had only Western-linked systems received the malicious updates? Beijing followed with its own accusations, claiming the United States had leaked its own tools to create a
plausible scapegoat. Their analysts traced the command servers to U.S. university research networks with a long history of intelligence use. “Coincidences,” Chinese outlets declared, “become patterns when repeated often enough.”

Adding to the chaos, a leak surfaced one day before the blackout: documents suggesting a secret meeting between Vladimir Putin and Kim Jong-un aboard a Russian icebreaker. No photographs, only flight plans and encrypted call signs, but enough to ignite speculation about a Russia–North Korea cyber alliance.
Meanwhile, Indian investigators uncovered a fragment of code buried in the malware, a failsafe program from an abandoned NATO, Russian joint project dating back to the Snowden era. Was it a forgotten relic, or a fingerprint planted to shift suspicion?

From Dubai, a new voice emerged. A self-proclaimed insider calling themselves KHORASAN began leaking fragments of satellite command packets and malware code. Independent labs across Europe and Asia confirmed the material was authentic, but incomplete. Enough to implicate every major power, never enough to exonerate anyone.
In encrypted correspondence with journalists, KHORASAN claimed to have worked on a multinational contractor team embedding “contingency controls” into satellite and grid systems under the pretense of counterterrorism. Those controls, they said, had later been sold to an “inside buyer with a grudge.” The blackout was not an attack but a demonstration. “What you saw was two percent,” they warned. “The rest is still sleeping in your systems.”

As the pieces came together, investigators realized they were not chasing a single virus but a long, deliberate infiltration. Over three years, it had mapped rail networks, airport communications, banking systems, and satellite firmware. It had not only compromised the technology, but studied how humans reacted to alerts, who had the authority to override, and how crises escalated across borders. When it finally activated, dashboards glowed green while critical systems failed. Engineers stared at healthy systems while their infrastructure collapsed in silence.
The stolen $2.1 billion was not the objective. It was proof of access, and perhaps the seed money for what comes next.

Now the world struggles to resume its routines. Lights are back, networks hum, markets open cautiously. But trust has fractured. Moscow points to Washington. Washington blames Moscow and Beijing. Beijing directs suspicion back across the Pacific. India doubts its own allies. The alleged Putin–Kim meeting lingers online. The NATO-era code fragment remains unexplained. And KHORASAN's final message hangs in the air: the blackout was only a rehearsal.
Every "all-green" console in the world is now a question mark.

WELCOME TO THE FCC

The 21st century is wired together by ambition. Nations built their economies, their defenses, and even their identities on the fragile pulse of digital networks. Fiber-optic cables snaked under oceans like lifelines; satellites blinked across orbit, guiding planes, trades, and wars alike. But in chasing speed, I guess, the world forgot how easily connection can become vulnerability.

The first real shock came in 2007, when Estonia fell victim to a massive DDoS (Distributed Denial-of-Service) attack. Following a diplomatic dispute with Russia over the relocation of a Soviet war memorial, Estonian banks, media outlets, and government systems were overwhelmed and shut down. It wasn't bombs or soldiers that silenced a nation, but traffic. Millions of fake requests crashing its digital heartbeat.

Then came Stuxnet, the first cyberweapon built not to steal, but to sabotage. Developed in secret by the United States and Israel, its code crept silently through the digital shadows for years. Researchers later traced its earliest variants to as far back as 2005, with its most destructive phase unfolding between 2009 and 2010. Inside Iran's Natanz nuclear facility, Stuxnet caused uranium centrifuges to spin wildly out of control, crippling Iran's nuclear program without firing a single shot. The world had entered an era where wars could be fought invisibly.

In 2015, the lights went out in Ukraine. Hackers believed to be linked to Russian intelligence infiltrated the power grid, shutting down substations and plunging hundreds of thousands into darkness. It was the first confirmed cyberattack to take down an entire national power system. This was proof of a concept that electricity itself could be weaponized.

The chaos multiplied as the years went on. In 2017, the NotPetya malware, initially disguised as ransomware, it spread from Ukrainian networks to the world. It crippled shipping giant Maersk, pharmaceutical company Merck, and even parts of Russia itself. Analysts estimate the total damage exceeded $10 billion, making it the most financially destructive cyberattack in history.

That same year, Trisis targeted a Saudi Arabian petrochemical plant, going after the safety controllers designed to prevent industrial accidents. For the first time, a cyberattack wasn't just about disruption. It aimed to cause physical destruction, possibly loss of life. Western intelligence later linked the malware to a Russian government research institute, marking another escalation in the invisible arms race.

By 2020, the SolarWinds supply-chain breach exposed the fragility of trust itself. A routine software update from the Texas-based IT company SolarWinds was secretly modified, giving hackers (believed to be Russian state actors) a backdoor into thousands of networks, including U.S. federal agencies like the Department of Homeland Security and parts of the Pentagon. The infiltration lasted for months before being discovered, proving that even the world's most secure systems could be compromised from within.

Meanwhile, as geopolitical tensions rose, attention shifted skyward. The increasing militarization of orbit and growing threats to satellite cybersecurity became clear by the early 2020s. Several space agencies and private operators reported isolated incidents of signal interference, spoofing, and attempted data breaches, though no large-scale, confirmed cyber conflict in orbit has occurred to date. The prospect, however, remains deeply alarming, an open frontier for the next generation of digital warfare.

These cascading crises made one thing undeniable: the world's dependence on digital infrastructure was total, and its defenses were dangerously fragmented. There was no global body capable of coordinating a unified response to a communication blackout or cyber-catastrophe.
And so, the Federal Communications Crisis Council (FCC Council) was formed, not as a traditional UN body, but as a coalition of international governments, private-sector partners, and cyber-defense agencies. Its purpose? To stand guard when the world's networks fall silent, to restore connection when chaos fractures the grid, and to ensure that when the next line of code turns deadly, humanity is ready.

BLUEPRINTS FROM THE PAST

UN Group of Governmental Experts (GGE) on ICTs

The UN GGE and the Open-Ended Working Group (OEWG) are the principal multilateral bodies addressing cybersecurity norms. They successfully established a consensus that international law, including the UN Charter, applies to cyberspace.

- Core Achievement: The groups agreed upon 11 voluntary, non-binding norms of responsible state behavior. These include directives to protect critical infrastructure, respond promptly to requests for assistance, and refrain from using proxies to commit malicious cyber activity.
- Limitation: Because these norms are voluntary and politically binding only in principle (not legally enforceable like a treaty), they do not prevent major powers from simultaneously developing and deploying offensive cyber capabilities. This parallel action undermines the goal of restraint and makes verification of compliance nearly impossible.

Regional Disaster Preparedness Programs

- ASEAN's Digital Resilience: ASEAN relies on the Cybersecurity Cooperation Strategy (CCS) 2021-2025 and the ASEAN Digital Masterplan (ADM) 2025. These focus on capacity building (training cyber response teams like CERTs) and information sharing among member states.
- EU Civil Protection Mechanism (EUCPM): The EUCPM is the framework for coordinated assistance during crises. While the Emergency Response Coordination Centre (ERCC) plays a role in crisis response, the mechanism's primary focus, resource allocation, and logistics (e.g., medical supplies, flood response) are designed for localized, physical disasters. Its contingency planning often fails to scale for the complexity of a cascading, transnational cyber system failure.

Private Tech Sector Initiatives

- Redundancy Technology: Projects like SpaceX's Starlink utilize massive constellations of Low-Earth Orbit (LEO) satellites connected by laser-based inter-satellite links to create a self-healing mesh network in space. This provides remarkable communication redundancy, especially in war zones or disaster areas where ground infrastructure fails.
- Limitation: These powerful systems are siloed commercial assets. They are not fully integrated into sovereign military or civilian emergency frameworks. Their operation is subject to corporate policy, making them an excellent source of redundancy but a poor substitute for coordinated, governed global policy.

Cybersecurity Exercises and War Games

NATO and multinational groups conduct extensive simulations, which are essential but limited in scope.

- Key Exercises: NATO's Locked Shields (organized by the CCDCOE) is the world's largest live-fire cyber defense exercise, focusing on defending critical infrastructure like power plants and military systems in real-time. Cyber Coalition focuses more on procedural, legal, and political coordination during a crisis.
- Limitation: While highly technical, these exercises rarely model simultaneous, multi-continent failures spanning financial markets, global shipping, and satellite communications all at once. They tend to focus on the immediate technical response rather than the full systemic collapse and cascading societal effects of a "full spectrum" digital crisis.

WHAT NOW?

At this stage, we understand that some of you might be feeling a bit uncertain about the next steps, wondering where to go from here, which angle to pursue, and what exactly you should be focusing on. Allow us to clarify how things will proceed from this point forward.

The topic we have provided is intentionally broad and somewhat open-ended. It reflects a real-world scenario that is still developing and leaves room for interpretation. Your role as delegates is to analyze the situation as it currently stands and determine what you believe may have happened next. From here on, any moderated or unmoderated caucus topics should be framed around your interpretation of the unfolding events and the possible outcomes that follow.
To assist you in this process, we will be releasing a series of leaked exposés. They will be documents that offer varying perspectives on what might have occurred behind the scenes. These leaks are meant to serve as clues or prompts to help guide your discussions and shape your narrative. You are encouraged to draw from these materials to strengthen your arguments, but you are by no means limited to them.

You are also free to develop your own theories or narratives, provided that they are supported by logical reasoning and evidence that you can present convincingly. Because this is a crisis council, events will evolve quickly, and the situation will remain fluid and dynamic. Your responses and the directions you choose to take will directly influence how the scenario develops. There is no fixed or predetermined outcome, the conclusion of this crisis will depend entirely on your actions, your diplomacy, and the arguments you bring forward.

In short, the next phase is now in your hands. The narrative will move forward based on the collective decisions and strategies of this committee. Be creative, be analytical, and above all, be prepared to adapt as the situation unfolds.

POSSIBLE UNMODERATED AND MODERATED CAUCUS TOPICS

MODERATED CAUCUS TOPICS

- How should nations respond when attribution in cyberwarfare is uncertain?
- Influence of private cooperations, shell companies and whistleblowers in this crisis.
- A geopolitical deep dive into the alleged Putin-kim meeting. Was it real, and if so, how does it tie into the blackout?

UNMODERATED CAUCUS TOPICS

- Should KHORASAN be protected and recruited, or silenced?
- Should the Blackout Be Classified as an Act of War?
- Should the $2.1 Billion Trail Be Publicly Exposed?

BIBLIOGRAPHY

http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/

https://ics.sans.org/media/E-ISAC-SANS-Ukraine-DA-Public-Report-18Mar2016.pdf

https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

https://cloud.google.com/blog/topics/threat-intelligence/attackers-deploy-new-ics-attack-framework-triton

https://www.cisa.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf

https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf

https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr937.pdf

https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-

https://cloud.google.com/blog/topics/threat-intelligence/attackers-deploy-new-ics-attack-framework-triton

https://docs.un.org/en/a/68/98

https://docs.un.org/en/a/70/174

https://asean.org/wp-content/uploads/2021/09/ASEAN-Digital-Masterplan-EDITED.pdf

https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/eu-civil-protection-mechanism_en

https://www.starlink.com/technology

https://aerospace.org/sites/default/files/20205/FY23_12205_SOP_Lasercom%20Ppr_r10.pdf