

Security Council (MS)

Topic: “Addressing State-Sponsored Cyberattacks Against Critical Infrastructure: Strengthening International Peace and Security ”

Written by: Sofía García Martínez

Writer's note:

Welcome delegates to the Security Council of LIMUN 2027. We are thrilled to have you here at this edition of the United Nations. This is one of the most important organs that the UN has so be prepared for great debates. As this is of the most recent topics worldwide there won't be as much information that is why we advise you to take a look at the “Question to Consider” segment in this background to help you. Remember you will have to investigate and debate according to your respective nation. Once again welcome, and good luck!

I. COMMITTEE BACKGROUND

The United Nations Security Council was established in 1945 following World War II to succeed the League of Nations and maintain international peace and security. The Council held its inaugural meeting on January 17, 1946, at Church House in London. It was granted the power to issue binding resolutions, impose sanctions, and authorize military action. Five victorious powers from World War II the United States, the Soviet Union, the United Kingdom, China, and France became the permanent members with veto power. Britain advocated for France to add a European voice, and the Soviet Union agreed because France might balance U.S. influence.

II. HISTORY OF THE TOPIC

a. Introduction of the topic

State-sponsored cyberattacks against critical infrastructure involve government-backed actors using advanced persistent threats (APTs) to disrupt, damage, or pre-position inside essential services like energy, water, and transportation. Many water and power facilities rely on remote-access tools or PLCs with weak passwords and direct internet exposure.

b. Evolution of the topic

State-sponsored cyberattacks against critical infrastructure remain a top national security concern, with recent Cybersecurity Dive reports showing nearly 90% of state technology leaders view these threats as a major risk. Municipal water systems in multiple states faced active targeting, leading agencies to urge manual fail-safes. According to an Industrial Cyber report, state authorities lack sufficient funding and staff to properly defend local water, energy, and health sectors.

c. Relevant Events

Water and Power Sectors:

Suspected Iranian-nexus and other state-backed hackers have targeted internet-exposed industrial control systems across multiple U.S. states, causing pressure loss and operational concerns.

China-Linked Operations:

State-sponsored groups like QTFY have utilized compromised IoT devices and commercial proxy infrastructure to pre-position themselves inside critical networks, leading to recent U.S. Department of Justice and FBI domain seizures.

Geopolitical Escalation:

State-backed campaigns in regions like Ukraine have seen massive surges in destructive malware, phishing, and continuous attempts to disrupt defense and energy operations.

III. CURRENT ISSUES

a. Panorama

The resolution will be centered on the issue of increasing danger from cyber-attacks against vital infrastructure of a nation such as hospitals, electrical grids, financial institutions, transportation services, telecommunications and water services that may be carried out by states. It could pose great threats to national security through disruptions to vital services, economic loss, social unrest and even threat to global peace and security. The delegates will look into ways of how to prevent or react to a cyber-attack that could be perpetrated by any state or under the patronage of a state. The challenge to this will include identification of the perpetrator, sovereignty of a nation and when it poses an international threat.

b. Points of View

China (PRC):

Engages in malicious cyber activities to pursue its national interests including infiltrating critical infrastructure networks. Governments including the United States, the United Kingdom, and their Five Eyes allies explicitly state that the People's Republic of China (PRC) sponsors malicious cyber operations targeting critical infrastructure networks worldwide. Conversely, the Chinese government consistently denies these allegations. Beijing routinely states that the accusations are politically motivated fabrications and claims that China itself is a frequent target of foreign cyber attacks and espionage operations.

Russia:

Engages in malicious cyber activities to enable broad-scope cyber espionage, to suppress certain social and political activity, to steal intellectual property, and to harm regional and international adversaries. Russian intelligence agencies, specifically the SVR (Foreign Intelligence Service), the GRU (Military Intelligence), and the FSB (Federal Security Service), regularly deploy highly sophisticated Advanced Persistent Threat (APT) groups. Cyber tools are frequently used by the Russian government to police dissent, monitor political opposition, and control the narrative both domestically and in near-abroad states.

Iran:

Has exercised its increasingly sophisticated cyber capabilities to suppress certain social and political activity, and to harm regional and international adversaries. This specific assessment is a core finding detailed by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and other Western intelligence agencies. Iran's cyber operations bridge the gap between domestic totalitarian survival and aggressive international asymmetrical warfare. Despite dealing with aggressive counter-cyber campaigns and kinetic strikes to its own physical command centers by Western forces, Iran continues to adapt by leveraging satellite connections and commercial malware markets to sustain its offensive digital operations

North Korea:

Employs malicious cyber activity to collect intelligence, conduct attacks, and generate revenue. State-sponsored hacking groups have stolen billions of dollars in digital assets from global crypto exchanges and decentralized finance (DeFi) platforms to directly fund the regime's nuclear and ballistic missile programs. While revenue generation is a massive priority, North Korea has also launched highly disruptive attacks, such as the infamous 2014 Sony Pictures hack and the 2017 global WannaCry ransomware outbreak.

IV. UN & EXTERNAL ACTIONS

a. UN

Through consensus reports by the UN Group of Governmental Experts (GGE) and the Open-ended Working Group (OEWG), the UN established that states should not conduct or support ICT activity that intentionally damages critical infrastructure providing services to the public. Member states affirm that existing international law, including the UN Charter and state sovereignty rules, fully applies to cyberspace. Following the conclusion of the OEWG mandate, the UN advanced discussions toward establishing a permanent, regular institutional dialogue mechanism to coordinate global cybersecurity threats, measure cyber harms, and build transparency.

b. External actions

Governments and agencies are implementing proactive operational disruptions, artificial intelligence integration, and whole-of-state funding frameworks to combat state-sponsored cyberattacks against critical infrastructure.

Domain Seizures:

Law enforcement agencies are actively dismantling malicious infrastructure. For example, the U.S. The Department of Justice and the Federal Bureau of Investigation (FBI) executed court-authorized seizures of hacking platforms like QScan and QTRouter used by state-sponsored Chinese groups.

AI-Enabled Defense:

Agencies are deploying artificial intelligence tools to triage massive datasets, map adversary infrastructure, and accelerate malware analysis at speeds humans cannot match.

State-Level Grants:

Local governments are rolling out financial support, such as New York's grant allocations for water utilities and Texas's Project Watershed 250 pilot, to secure under-resourced local infrastructure.

V. CONCLUSION

Cyberattacks by states on critical infrastructure constitute a new threat to peace and security on an international level. In the modern age of increased reliance on computer networks, attacks on crucial sectors, including energy, healthcare, transport, communication, water, and finance, have implications far beyond the virtual world. Moreover, involvement of state actors makes the problem even more complicated since it raises a number of very sensitive questions regarding the attribution of actions, protection of national sovereignty, and appropriate response.

However, while the international community recognized the applicability of international law to cyberspace and the non-destructive nature of state actions towards critical infrastructure, a number of problems still exist. The attribution of cyberattacks may be complicated, the levels of cybersecurity development are very diverse among different countries, and international frameworks for cyberspace development and protection from attacks evolve at the same time as technological changes occur.

Thus, the Security Council should think about ways of strengthening cooperation, information exchange, securing vulnerable infrastructure, and appropriate measures to take after significant cyberattacks. Delegates are to examine the role of the international community in addressing the problem of state-sponsored attacks on critical infrastructure and ways in which the international community can cooperate.

VI. QUESTIONS TO CONSIDER

1. What is a cyberattack sponsored by a state, and how does it differ from cybercrime or an attack carried out by non-state actors?
2. Which types of critical infrastructure are vulnerable to cyberattacks?
3. Why is a state-sponsored cyberattack now regarded as a threat to international peace and security?
4. What would be the consequences of an attack on energy grid infrastructure, healthcare systems, banking systems, communications networks, transportation systems, etc?
5. In what case could a cyberattack be an infringement of the sovereign right of a state?
6. Under what circumstances could a cyberattack be considered as an “armed attack” or “use of force”?
7. How should the international community respond if there is a suspicion of state sponsorship of the cyberattack but the responsible party cannot be determined for sure?
8. What is already in place in terms of international law and relevant UN principles and resolutions?
9. How could the states collaborate in exchanging information and sharing intelligence to prevent a cyberattack?
10. What should be the role of the UN and Security Council in the case of significant cyberattacks?

VII. REFERENCES

What Is the UN Security Council? (2024, 10 November). CFR Education.

<https://www.cfr.org/education/learn/reading/what-un-security-council>

Check Point Software Technologies Ltd. (2026, 12 August). *Check Point Software:*

Leader in Cyber Security Solutions. Check Point Software. <https://www.checkpoint.com/>

Department of Justice | Homepage | United States Department of Justice. (2026, 8

September). <https://www.justice.gov/>

Cybersecurity News and Analysis | Cybersecurity Dive. (n. d.).

<https://www.cybersecuritydive.com/>

Interface — Tech analysis and policy ideas for Europe. (n. d.). Interface.

<https://www.interface-eu.org/>

The Student Strategy & Security Journal | An Student-Led academic journal. (n. d.).
<https://3sjournal.com/>

Protect.ngo | protect.ngo. (n. d.). <https://protect.ngo/>

Boston Herald. (n. d.). Boston Herald. <https://www.bostonherald.com/>

Fox-Sowell, S. (2026, 10 septembre). States confront growing cyber gaps as critical infrastructure threats rise, report finds. *StateScoop*.
<https://statescoop.com/states-confront-growing-cyber-gaps-as-critical-infrastructure-threats-rise-report-finds/>

(n.d.). NJCCIC | Home NJCCIC. Retrieved September 16, 2026, from
<https://www.cyber.nj.gov/>

(2021, September 2). The Heritage Foundation. Retrieved September 16, 2026, from
<https://www.heritage.org>

(2026, janaury 23). The International Institute for Strategic Studies. Retrieved September 16, 2026, from <https://www.iiss.org/>

(2026, September 11). Industrial Cyber Security Solutions - OT/ICS, SCADA Cyber Security System. Retrieved September 16, 2026, from <https://industrialcyber.co/>

Nation-State Threats | Cybersecurity and Infrastructure Security Agency CISA. (n.d.). CISA. Retrieved September 16, 2026, from
<https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors>