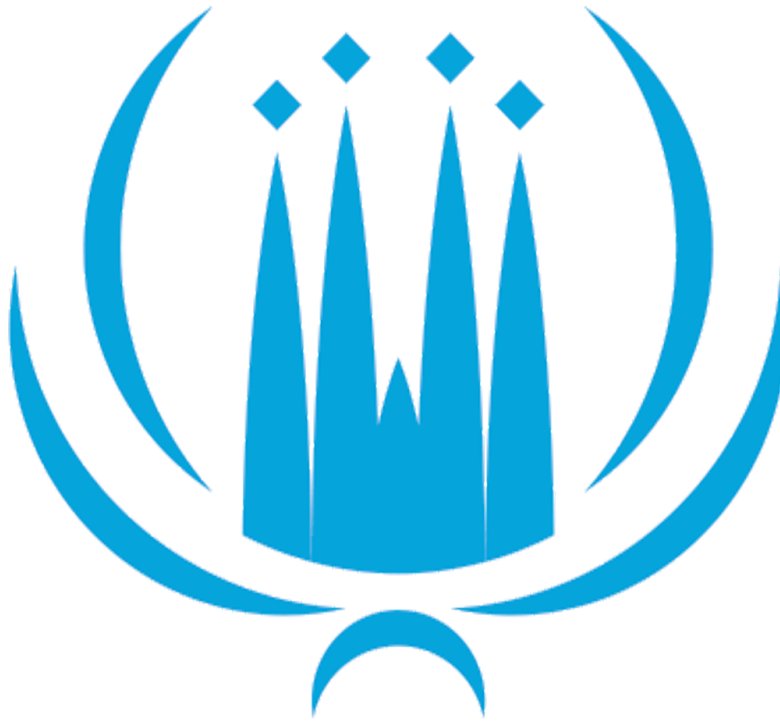




Security Council

BCNMUN 2026

From Crisis to Cooperation:
Navigating Instability in a Globalized World

Table of Contents

Table of Contents.....	1
Introduction.....	2
Definition of Key Terms.....	3
Background Information.....	3
Major Countries and Organisations Involved.....	5
Timeline of Events.....	6
Relevant UN Treaties and Resolutions.....	6
Previous Attempts to solve the Issue.....	7
Possible Solutions.....	7
Bibliography.....	7

Topic: Addressing the effects of state-sponsored international espionage and its threat to international peace and security.

Chair: Nils Leijdekker

Position: Expert Chair

Introduction

Espionage has existed as long as there have been people or groups to spy on; it is often called “the world's second-oldest profession” for this reason. It goes to show just how engrained in our existence the idea of gathering intelligence is. Humans have naturally always sought out information, particularly if that information is being withheld from them. For centuries people have tolerated this behavior as a “below the threshold of war” activity: something that isn’t worthy of declaring war necessarily, but is also not very peaceful. Espionage as an issue is different from others because it is something that has always happened, but what has changed is the way people conduct it. The tool changed, not the behavior. In modern warfare, new cyber technology allows states to spy on others without ever crossing a border, which creates deniability and desensitization.

State-sponsored espionage is the state-authorized gathering of intelligence directed at another state's government, companies, or citizens. There are three major types of espionage: political/military espionage, economic/industrial espionage, and the newest (and perhaps most dangerous) type, cyber espionage. These will be defined in the Definition of Key Terms. States can also conduct proxy espionage, where they will hire private organizations to conduct this espionage, which is dangerous because it adds yet another layer of deniability that states can hide behind.

This deniability has allowed states to be far more reckless in their espionage, incentivizing them to go further and conduct missions they would have never thought possible or reasonable. These actions can very easily escalate conflicts, in some cases to the brink of open conflict. The issue arises with the fact that there is no concrete UN law prohibiting this behavior. In fact, scholars are even in debate about whether it should be banned or not.

Definition of Key Terms

Espionage

The act of secretly gathering information from a government or organization without authorization.

Political/Military Espionage

The gathering of political/military secrets, military capabilities, alliances, and plans from another nation.

Economic/Industrial Espionage

The gathering of trade secrets, technology, or corporate data; normally for a competitive advantage.

Cyber Espionage

This involves both intelligence gathering and infrastructure intrusions, except it utilizes technology to do this much more efficiently, effectively, and (often) remotely.

Attribution

The process of identifying which state, organization, or individual is responsible for committing a crime, such as espionage.

Soft law

Soft law is a rule that states will have agreed to in theory, for example, in the form of a resolution, but do not actually follow due to a lack of enforcement.

Proxy Actor

An organization that will carry out espionage on another state or organization on behalf of another state or organization.

Background Information

Historical Background Information

Espionage has been used by states for millennia, but only in the Cold War did it become entangled enough with modern warfare and legal order to be brought to the United Nations. In this time, state intelligence agencies like the CIA, KGB, and MI6 ran espionage as a core part of their strategy, essentially becoming institutionalized. Human intelligence, reconnaissance fighters, and networks of defectors all played a large role in this conflict. Despite all of this espionage, both sides were still highly against the opposing side doing so. One instance of this was the infamous U-2 incident. After being caught in an act of espionage, the US faced absolutely zero legal consequences, even after the matter was taken to the Security Council. This incident from 1960 is illustrative of the lack of accountability. This form of espionage had become essentially a tolerated norm of warfare. Just as people accept that people will die in war, it seemed as if in that time, people had come to the conclusion they were okay with the idea of espionage in war.

After the Cold War, however, the purpose of espionage changed. During the war, intelligence agencies were mainly trying to get information on their enemy and learn military and political secrets. After the collapse of the Soviet Union, many governments switched their intelligence forces to focus on primarily economic competition. This was because of a few factors, but largely power came increasingly from wealth, not pure military prowess. Given the threat of nuclear war was extinguished, nations could focus on growing their economies, which meant that they became increasingly dependent on technology for those economies. Instead of wondering how many missiles the enemy had, they were now wondering about the technological capabilities of their adversaries and how they could get a leg up. As a result, intelligence agencies increasingly collected more trade information, energy data, financial intelligence, and more. This became known as economic espionage.

Then, after the turn of the century, espionage changed once more. It became digital. For centuries, gathering information meant intercepting signals or physically sending spies to learn information. Initially, cyber espionage followed this trend by focusing on stealing data. However, this changed with Stuxnet.

Stuxnet was a highly advanced computer virus that was developed by the United States and Israel in the 2000s. Unlike previous malware, Stuxnet was never designed to steal information or disrupt computers; it was instead trying to sabotage the uranium enrichment factories in Iran. It was designed to work slowly and sit undetected for as long as possible. All it would occasionally do was slight damage to the centrifuges, leading them to eventually all fail. The most innovative aspect was not the sabotage that it caused, but the deception it used. It was able to mask its actions perfectly, so it seemed as if nothing was wrong to the operators. What made it special was that it caused real physical damage while not a single soldier ever had to cross a border. They could cause harm from the safety of their own home. This is the crux of how cyber espionage became a UN concern and no longer a minor diplomatic annoyance.

Current Situation in the World

After 21 years of negotiation, the UN's cyber norms process finished its last cycle in 2025, as it is now being replaced with a new permanent mechanism. Despite all of this negotiation and diplomacy, many analysts have noted that the final report has broken very little new ground beyond the original 11 norms that were agreed upon in 2015, and that was purely soft law. And in addition to this, the Security Council has never adopted a resolution specifically addressing cyber/espionage operations, despite two decades of discussion. And incidents such as Stuxnet are still happening. In 2020, Russian intelligence hacked into SolarWinds, an American company that makes software for business management. This gave them a back door to roughly 18,000 organizations, including multiple US federal agencies. This event is interesting, as scholars are still split on whether or not this was even illegal. Some argue that it violates states' "due diligence" obligations, while others call it the "espionage of the sort the US itself excels at, not an act of war." Even today, this is still in a legal gray zone, making it impossible to even begin convicting actions such as this. There have never been any UN resolutions that concretely covered the topic of espionage and came to a concrete binding conclusion. This has made this 'gray zone' more like an anarchy zone, where it seems as if everything is allowed.

Major Countries and Organizations Involved

The United States

The United States has a very long history of carrying out espionage both in and outside of warfare. They have been responsible for some of the largest and most damaging acts of espionage in history, such as Stuxnet, Nitro Zeus, Duqu and Flame, and more.

Russia

Russia is also infamous for their espionage and overall cybercrime, with them being linked to the infamous SolarWinds incident and the GRU attacks against Georgia.

Iran

Iran was the victim of the Stuxnet attack; they lost nearly 1,000 centrifuges to the operation, which delayed their nuclear program by an estimated 2 years. They are an example of a nation suffering real, physical loss from an attempt at espionage/sabotage.

People's Republic of China

The People's Republic of China is also an example of a nation that conducted damaging and intrusive espionage. They were attributed to the operation of the Salt Typhoon campaign, which breached major US and Canadian telecommunications providers and stole call records and private communications, including those of government officials. Some reports also attribute them to widespread stealing of trade secrets and economic espionage.

Israel

Israel has also expressed its willingness and capability to carry out devastating espionage operations, the most famous of which being Stuxnet. It has an elite military intelligence branch known as Unit 8200, which has a pipeline which creates some of the most advanced commercial spyware in the world.

Five Eyes (FVEY)

Five Eyes is an intelligence-sharing alliance between the US, UK, Australia, New Zealand, and Canada. It is a multilateral organization that cooperates on signals intelligence, cybersecurity, and global surveillance.

NSO Group

The NSO Group is an Israeli spyware company that was responsible for the development of Pegasus, which was a powerful spyware designed to infiltrate phones and extract personal data, track locations, and operate cameras and microphones without the user knowing.

Timeline of Events

Date	Description of Event
May 1st, 1960	U-2 Incident A US spy plane was shot down over Soviet territory, and the pilot, Francis Gary Powers, was captured and tried for espionage. Eisenhower first claimed that the plane was a high-altitude weather aircraft that had flown off course, but the Soviets revealed that they also found the wreckage of the plane, which proved it was a spy mission.
May 16-17, 1960	Collapse of the Paris Summit Khrushchev walked out of the Paris Summit after Eisenhower refused to apologize for the U-2 flight, which ended the summit before any talks could occur, leading to a lack of crucial de-escalation that could have happened.
May 23-27, 1960	Soviet Taking Complaint to the Security Council The Soviet Union brought the U-2 Incident to the Security Council, but their resolution was rejected, and a competing Western resolution was passed instead, leading to no binding consequence for the United States to follow.
1990s	Shift Towards Economic Espionage After the collapse of the Soviet Union, state intelligence agencies moved away from targeting military agencies and instead focused on targeting trade secrets, technology, and economic data as national power became increasingly tied to

economic strength instead of military prowess.

December 2015

GGE Reaches Consensus on 11 Cyber Norms

The UN Group of Governmental Experts came to an agreement on 11 non-binding norms of responsible state behavior in cyberspace, which were later endorsed by the General Assembly. This is still the high-water mark of UN cyber negotiations despite them being entirely nonbinding and over a decade old.

July 11, 2025

OEWG Adopts Final Report

After a cumulative 21 years of UN cyber negotiations, the OEWG concluded, yet analysts noted how it “broke little new ground” beyond the norms set in 2015. A new global mechanism was established to continue negotiations, though espionage itself remains outside its explicit scope.

Previous Attempts to Solve the Issue

There have been various attempts to solve the issue of espionage, but most have been temporary treaties for a specific conflict, and very few have had anything to do with the UN. One such treaty was the 2015 US-China Cyber Agreement, when Barack Obama and Xi Jinping agreed that neither government would “conduct or knowingly support cyber-enabled theft of intellectual property (...) for commercial advantage.” Critics believe the issue with this agreement was that it explicitly did not cover political/military espionage by cyber means, only commercial theft, leaving a gap in the 'solution,' as it ignored the bulk of the issue.

In general, diplomatic and legal methods have been used by nations to discourage espionage; in 2014, the US indicted 5 PLA (People's Liberation Army) officers for cyber espionage. This was a largely symbolic action, as the US knew China would refuse their extradition, but it reportedly was effective as pressure. Prisoner exchanges have also been used but to limited success, as it makes it easier for spies to

go undercover, as it gives them the safety net of knowing they have a way back home if something were to go wrong.

Possible Solutions

The Creation of an Attribution Mechanism

One of the largest issues faced is the lack of a way to prove that a nation engaged in espionage. The creation of an independent, technical body that states could refer suspected operations to for a neutral, third-party assessment would greatly improve the ability to prove what a state did or did not do.

A Framework for Conviction

The second large issue is that there has been no strict definition of what is and isn't allowed in the world of espionage. There has never been an SC resolution about espionage or any agreement that is legally binding. Therefore, the most important actions would be passing a resolution defining what is actually illegal by international law and what the punishments are for illegal espionage. These consequences have been hinted at but never properly specified in a binding format.

Closing the Proxy-Actor Loophole

It would also be useful to build off of the 2015 GGE paragraph 28(e), which stated that “states must not use proxies (...) should ensure territory isn't used by non-state actors.” Enforcing this with due diligence reporting obligations or a registry/licensing requirement for commercial spyware companies would go a long way towards closing this crucial loophole.

Bibliography

1. “Foreign Relations of the United States : May - July 1960 : The U-2 Airplane Incident - Editorial Note.” *Avalon Project*, avalon.law.yale.edu/20th_century/vx147.asp. Accessed 8 July 2026.
2. *Milestones in the History of U.S. Foreign Relations - Office of the Historian*, history.state.gov/milestones/1953-1960/u2-incident. Accessed 8 July 2026.
3. *The Real Story of Stuxnet - IEEE Spectrum*, spectrum.ieee.org/the-real-story-of-stuxnet. Accessed 8 July 2026.

4. Lewis, James A. "UN Norms: Tackling the Rise of Cyber Capabilities | Royal United Services Institute." *Rusi*, 31 Mar. 2026, www.rusi.org/explore-our-research/publications/commentary/un-norms-tackling-rise-cyber-capabilities.
5. Temple-Raston, Dina. "A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack." *NPR*, 16 Apr. 2021, <https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack>. Accessed 7 July 2026.
6. "U.S., China Say They Won't Engage in Cybertheft." *CNN*, 25 Sept. 2015, www.cnn.com/2015/09/25/politics/us-china-cyber-theft-hack/index.html. Accessed 12 July 2026.
7. "A New Old Threat: Countering the Return of Chinese Industrial Cyber Espionage." *Council on Foreign Relations*, www.cfr.org/report/threat-chinese-espionage. Accessed 12 July 2026.
8. "Why the SolarWinds Hack Is a Wake-Up Call." *Council on Foreign Relations*, www.cfr.org/article/why-solarwinds-hack-wake-call. Accessed 12 July 2026.
9. "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System." *Cybersecurity and Infrastructure Security Agency*, cisa.gov/news-events/cybersecurity-advisories/aa25-239a. Accessed 12 July 2026.
10. United Nations General Assembly. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174, 22 July 2015, documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf. Accessed 12 July 2026.
11. United Nations General Assembly. *Developments in the Field of Information and Telecommunications in the Context of International Security*. A/RES/70/237, 30 Dec. 2015, digitallibrary.un.org/record/814504. Accessed 12 July 2026.