

HMDC Presents... LEGAL: Part 2 (The United Nations)

HMDC Presents... Legal Committee (Sixth Committee): Cyberwarfare Case Studies (Research Report, December 2026)

WHAT OUR CHAIRS WILL FOCUS ON

Harvard tells us that this committee looks at cyberattacks between countries and asks how the world can work together to answer them. In the December session, we will study real examples of cyberwarfare, which Harvard calls "an area of pressing potential threat." We will judge how much harm these attacks cause, and then we will build legal frameworks, meaning sets of rules, that make that harm smaller. (Harvard Model United Nations, HMUN Online Committee Page, Last Accessed: October 2026)

<https://www.harvardmun.org/legal-online>

The parts of this report that match that focus most closely are The Harms in Part 1 (our case studies), the four Solutions in Part 1 (our legal frameworks), and Where the Major Blocs Stand in Part 2.

How we use this report: Harvard says the October session covers cybercrime by criminal groups, and the December session covers cyberwarfare by countries. So we put most of our time into attacks by states, or by groups working for states, and into the law that applies to them. The entries about the UN Convention against Cybercrime and about ransomware gangs are background only, and we use them just to show that countries can agree on rules for cyberspace. We keep all of this research, but our speeches and resolutions should stay on cyberwarfare.

PART 2, THE UNITED NATIONS RECORD

The UN has worked on cyber security since 1998, mainly through the First Committee (security), which created expert groups and working groups. Separately, the Third Committee led work on cybercrime, which produced the first UN cyber treaty in 2024. The Sixth Committee's direct link is through the International Law Commission, which in 2025 began studying "due diligence," a principle very relevant to cyberspace.

UN Resolutions and Major Instruments

Only symbols confirmed on an official UN site (un.org General Assembly resolution lists, UNODA or UNODC pages) are listed. Most First Committee resolutions from 1998 to 2017 were the yearly resolution on "developments in the field of information and telecommunications in the context of international security"; the official page confirmed their symbols but did not describe each one separately.

Symbol	Year	Body	What it does
A/RES/53/70	1998	General Assembly (First Committee)	The first UN action on information security; introduced by Russia and adopted without a vote.

A/RES/54/49	1999	General Assembly (First Committee)	Continues the yearly resolution on information and telecommunications in international security.
A/RES/55/28	2000	General Assembly (First Committee)	Continues the yearly resolution on information security.
A/RES/56/19	2001	General Assembly (First Committee)	Continues the yearly resolution on information security.
A/RES/57/53	2002	General Assembly (First Committee)	Continues the yearly resolution on information security.
A/RES/58/32	2003	General Assembly (First Committee)	Continues the yearly resolution on information security.
A/RES/59/61	2004	General Assembly (First Committee)	Continues the yearly resolution on information security.
A/RES/60/45	2005	General Assembly (First Committee)	Continues the yearly resolution on information security.
A/RES/61/54	2006	General Assembly (First Committee)	Continues the yearly resolution on information security.
A/RES/62/17	2007	General Assembly (First Committee)	Continues the yearly resolution on information security.
A/RES/63/37	2008	General Assembly (First Committee)	Continues the yearly resolution on information security.
A/RES/64/25	2009	General Assembly (First Committee)	Continues the yearly resolution on information security.
A/RES/65/41	2010	General Assembly (First Committee)	Continues the yearly resolution on information security.
A/RES/66/24	2011	General Assembly (First Committee)	Continues the yearly resolution on information security.
A/RES/67/27	2012	General Assembly (First Committee)	Continues the yearly resolution on information security.
A/RES/68/243	2013	General Assembly (First Committee)	Continues the yearly resolution on information security.
A/RES/69/28	2014	General Assembly (First Committee)	Continues the yearly resolution on information security.
A/RES/70/237	2015	General Assembly (First Committee)	Continues the yearly resolution on information security, the year of the GGE report that set out voluntary norms.

A/RES/71/28	2016	General Assembly (First Committee)	Continues the yearly resolution on information security.
A/RES/73/27	2018	General Assembly (First Committee)	Creates the first Open-ended Working Group (OEWG), open to all UN members.
A/RES/73/266	2018	General Assembly (First Committee)	"Advancing responsible State behaviour in cyberspace"; creates the sixth Group of Governmental Experts (2019-2021).
A/RES/73/187	2018	General Assembly (Third Committee)	Addresses countering the use of information and communications technologies for criminal purposes.
A/RES/73/218	2018	General Assembly (Second Committee)	Addresses information and communications technologies for sustainable development.
A/RES/74/28	2019	General Assembly (First Committee)	One of two 2019 resolutions on ICT security.
A/RES/74/29	2019	General Assembly (First Committee)	The second of the two 2019 resolutions on ICT security.
A/RES/74/173	2019	General Assembly (Third Committee)	Promotes international cooperation and information-sharing to combat cybercrime.
A/RES/74/197	2019	General Assembly (Second Committee)	Addresses information and communications technologies for sustainable development.
A/RES/74/247	2019	General Assembly (Third Committee)	Creates the Ad Hoc Committee to write a cybercrime convention.
A/RES/75/240	2020	General Assembly (First Committee)	Creates the second, five-year OEWG on ICT security (2021-2025).
Decision 75/564	2021	General Assembly	Endorses the first OEWG's final report and recommendations.
A/RES/75/282	2021	General Assembly (Third Committee)	Sets the schedule for cybercrime treaty negotiations, starting in January 2022.
A/RES/76/19	2021	General Assembly (First Committee)	ICT security resolution adopted in 2021.
A/RES/76/189	2021	General Assembly (Second Committee)	Addresses information and communications technologies for

			sustainable development.
A/RES/77/37	2022	General Assembly (First Committee)	Starts work on a permanent "Programme of Action" to advance responsible state behaviour in ICTs.
A/RES/78/237	2023	General Assembly (First Committee)	Continues the yearly resolution on developments in information and telecommunications in international security.
A/RES/79/237	2024	General Assembly (First Committee)	Endorses the elements of the future Global Mechanism on ICT security set out in annex C of the third OEWG progress report (A/79/214).
A/RES/79/243	2024	General Assembly	Adopts the UN Convention against Cybercrime (December 24, 2024).
A/RES/80/16	2025	General Assembly (First Committee)	Endorses the second OEWG's final report (A/80/257) and asks the Secretary-General to support the Global Mechanism on ICT security from 2026.
A/75/816	2021	First OEWG (report)	Final report of the first OEWG, adopted by consensus in March 2021.
A/76/135	2021	Sixth GGE (report)	Final consensus report of the 25-member Group of Governmental Experts.
A/76/136	2021	Sixth GGE (compendium)	Collects national views on how international law applies to state use of ICTs.
A/80/257	2025	Second OEWG (report)	Final report of the 2021-2025 OEWG, which sets out further elements of the Global Mechanism.

Not in the table: 2017 produced only a First Committee draft (A/C.1/72/L.44) on the official UNODA list, so no 2017 resolution is shown. Resolution 79/237 is confirmed through its citation in the official text of A/RES/80/16; its own page could not be opened during this research.

UNODA ICT Security Page, Last Accessed October 2026

Tagline: Tracing UN cyber work since 1998

Source: According to... UN Office for Disarmament Affairs, Last Accessed: October 2026

Link: <https://disarmament.unoda.org/ict-security/>

Fact: It states... the UN first took up information security in 1998, through a resolution introduced by Russia. Since 2004, six Groups of Governmental Experts have studied the issue; four produced consensus reports, each building on the last. The work covers five areas: threats, how international law applies, norms of responsible state behaviour, confidence-building measures and capacity building.

This means... the UN has a long and steady record of agreement in principle, especially that international law applies in cyberspace. The open question for this committee is how it applies in specific cases.

UNODA GGE Page, Last Accessed October 2026

Tagline: Reaching consensus among 25 experts

Source: According to... UN Office for Disarmament Affairs, Last Accessed: October 2026

Link: <https://disarmament.unoda.org/group-of-governmental-experts/>

Fact: It states... the sixth Group of Governmental Experts, created by resolution 73/266, had 25 members, including China, Russia, the United States, India, Brazil and Kenya, and was chaired by Brazil. It produced a final report (A/76/135) and a compendium of national views on international law (A/76/136).

This means... rival powers can agree on a shared text when the group is small. The weakness is that 25 states do not speak for all 193 members.

UNODA OEWG Page, Last Accessed October 2026

Tagline: Opening talks to every member

Source: According to... UN Office for Disarmament Affairs, Last Accessed: October 2026

Link: <https://disarmament.unoda.org/open-ended-working-group/>

Fact: It states... the first Open-ended Working Group was created by resolution 73/27, chaired by Switzerland and open to all UN members, with meetings also for industry, NGOs and universities. It adopted its final report on March 12, 2021.

This means... the UN moved from small expert groups to talks open to all states. This is more inclusive, but it makes agreement harder.

UNIDIR Analysis, April 8, 2026

Tagline: Reviewing the second working group

Source: According to... United Nations Institute for Disarmament Research, April 8, 2026

Link: <https://unidir.org/analysing-open-ended-working-group-security-icts/>

Fact: It states... the second OEWG met in 11 sessions from December 2021 to July 2025, and more than 130 delegations spoke. It produced three yearly progress reports and a final report, which laid the foundation for a permanent body, the Global Mechanism on ICT security. Women reached equal participation as speakers from the sixth session onward.

This means... the UN now has a permanent forum for cyber security, replacing temporary groups. Delegates can propose that the Global Mechanism and the Sixth Committee share legal findings.

UNIDIR Event Page, July 21, 2026

Tagline: Launching the permanent Global Mechanism

Source: According to... United Nations Institute for Disarmament Research, July 21, 2026

Link: <https://unidir.org/event/launching-unidirs-report-on-the-open-ended-working-group-on-ict-2021-2025/>

Fact: It states... UNIDIR launched its study of the 2021-2025 OEWG on July 21, 2026, as a side event to the Global Mechanism on ICT security at UN Headquarters. The study maps which issues reached the consensus reports and which were left out.

This means... the Global Mechanism was meeting in mid-2026. Issues left out of past consensus reports, such as the precise application of the law of war, remain open for debate.

UNIDIR Commentary, June 24, 2026

Tagline: Studying due diligence at the ILC

Source: According to... United Nations Institute for Disarmament Research, June 24, 2026

Link: <https://unidir.org/due-diligence-in-early-practice-the-international-law-commission-agenda-and-cyberspace/>

Fact: It states... "due diligence" means a state should not knowingly allow its territory to be used to harm other states. The 2015 expert report made this a voluntary norm for cyberspace, and the 2021 report said it requires reasonable steps but not monitoring of all activity. In 2025 the International Law Commission added "due diligence in international law" as a topic, and its Special Rapporteur's first report (April 2026) discussed possible application to cyberspace. Some states say the rule is binding; others say it is voluntary.

This means... this is the most direct link between cyberwarfare and the Sixth Committee, which receives and debates the ILC's reports every year. Delegates can take a position on whether due diligence is binding in cyberspace.

UNODC Ad Hoc Committee Page, Last Accessed October 2026

Tagline: Negotiating the cybercrime convention

Source: According to... UN Office on Drugs and Crime, Last Accessed: October 2026

Link: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

Fact: It states... resolution 74/247 created an Ad Hoc Committee to write a convention on countering the criminal use of ICTs. Resolution 75/282 (May 26, 2021) set at least six ten-day negotiating sessions starting in January 2022. The final session was held in New York from July 29 to August 9, 2024.

This means... the UN can negotiate a binding cyber treaty in about four years. Delegates can use this as a model, or as a warning about how hard negotiations were.

UNODC Convention Page, Last Accessed October 2026

Tagline: Adopting the first cyber treaty

Source: According to... UN Office on Drugs and Crime, Last Accessed: October 2026

Link: <https://www.unodc.org/unodc/en/cybercrime/convention/home.html>

Fact: It states... the General Assembly adopted the UN Convention against Cybercrime on December 24, 2024. It was signed in Hanoi on October 25, 2025, stays open for signature until December 31, 2026, and enters into force once 40 states become parties. It has nine chapters, including human rights safeguards and international cooperation.

This means... the convention covers crime, not warfare between states. Delegates must decide whether a similar binding approach should be tried for state cyber operations, or whether that is unrealistic.

UN Press Release GA/12671, Last Accessed October 2026

Tagline: Recording divided views at adoption

Source: According to... United Nations Meetings Coverage and Press Releases, Last Accessed: October 2026

Link: <https://press.un.org/en/2024/ga12671.doc.htm>

Fact: It states... at the close of the main part of its 79th session, the General Assembly adopted the cybercrime convention. Russia's delegate called it the result of five years of work, said negotiations were tense, and wanted additional protocols. Viet Nam called it the first international legal instrument governing cyberspace.

This means... states see the convention differently: some want to expand it with more protocols, while others worry about human rights. These divisions will appear in any cyberwarfare debate.

UNIDIR Compendium, July 20, 2026

Tagline: Including gender in cyber policy

Source: According to... United Nations Institute for Disarmament Research, July 20, 2026

Link: <https://unidir.org/publication/mainstreaming-gender-in-cybersecurity-a-compendium-of-good-practices/>

Fact: It states... UNIDIR and the Stimson Center collected practices for including gender in cyber policy, covering how cyber threats affect people differently, how to interpret international law with the experiences of those affected in mind, and capacity-building that supports women in cyber fields.

This means... harm from cyber operations is not equal across groups. A resolution can include gender-sensitive language, which is now common in UN cyber texts.

UNIDIR Publication, September 18, 2026

Tagline: Extending cyber norms to AI

Source: According to... United Nations Institute for Disarmament Research, September 18, 2026

Link: <https://unidir.org/publication/from-cyberspace-to-ai-translating-norms-of-responsible-state-behaviour-in-cyberspace-to-ai-in-the-military-domain/>

Fact: It states... the voluntary UN cyber norms should not be copied directly to military AI but can guide those discussions. States increasingly agree that international law applies, that humans must control the use of force, and that civilians must be protected, but they still disagree on terms, red lines and whether rules should be voluntary or binding.

This means... the same split (voluntary norms versus binding law) runs through the UN record. What is working is agreement on principles; what is not working is agreement on binding detail.

UN General Assembly Resolution A/RES/80/16, December 1, 2025

Tagline: Starting the permanent Global Mechanism

Source: According to... United Nations General Assembly, December 1, 2025

Link: https://digitallibrary.un.org/record/4095875/files/A_RES_80_16-EN.pdf

Fact: It states... on the report of the First Committee, the General Assembly endorsed the final report of the 2021-2025 Open-ended Working Group (document A/80/257). It asked the Secretary-General to support the Global Mechanism on ICT security and responsible State behaviour starting in 2026, building on elements already endorsed in resolution 79/237. It also asked for a new online portal for cooperation and capacity building, and kept the topic on the agenda of the 81st session.

This means... the UN now has a permanent home for cyber security talks instead of short-term groups. The Sixth Committee can recommend that legal questions, such as what counts as an "attack," be sent to this permanent body for steady work.

UN Geneva, November 8, 2024

Tagline: Debating hospital ransomware at the Security Council

Source: According to... United Nations Geneva, November 8, 2024

Link: <https://ungeneva.org/en/news-media/news/2024/11/100103/cyberattacks-healthcare-global-threat-cant-be-ignored>

Fact: It states... the Security Council held a briefing on ransomware attacks against hospitals. WHO Director-General Tedros said these attacks "can be issues of life and death." One 2021 survey found that over one-third of health institutions had suffered at least one ransomware attack in the past year. The United States accused Russia of letting ransomware groups operate from its territory; Russia denied this and asked for the Cybercrime Convention to enter into force quickly, plus a new protocol to protect critical infrastructure. China said the topic belonged in more specialised forums.

This means... the most powerful UN body is divided on whether cyber harm to hospitals is its business. Delegates can use the Russian proposal for an extra protocol and the Western focus on safe havens to find shared ground on protecting health care.

Permanent Mission of Australia to the UN, July 22, 2026

Tagline: Regretting gaps in agreed law

Source: According to... Permanent Mission of Australia to the United Nations, July 22, 2026

Link: https://unmy.embassy.gov.au/unmy/260722_GM_International_Law.html

Fact: It states... at the first working session of the Global Mechanism, Australia noted that "All States have agreed that existing international law applies to State conduct in cyberspace," and that the 2025 final report recorded agreement on sovereignty, non-intervention, the ban on the use of force and the peaceful settlement of disputes. Australia regretted that the report left out other common ground, including how international humanitarian law applies, along with human rights law and state responsibility. It proposed testing the law against concrete cyber incident scenarios and helping more states write national positions.

This means... the law of war in cyberspace is the biggest gap in the UN record. Studying real incidents one by one, which is exactly what this committee does, is a method that states themselves are now proposing.

Government of Canada, July 16, 2026

Tagline: Counting slow treaty ratifications

Source: According to... Global Affairs Canada, July 16, 2026

Link: <https://www.canada.ca/en/global-affairs/news/2026/07/canada-signs-united-nations-convention-against-cybercrime.html>

Fact: It states... when Canada signed the UN Convention against Cybercrime on July 16, 2026, it joined 78 other signatories, including the European Union, but only three states had ratified. The convention takes effect once 40 states ratify. Canada said the treaty's human rights safeguards are among the strongest in any international criminal justice treaty.

This means... signing is quick, but ratifying is slow. Nine months after the signing ceremony in Hanoi, the treaty was still far from entering into force, which is a warning for anyone proposing a new cyberwarfare treaty.

Global Initiative Against Transnational Organized Crime, September 2026

Tagline: Stalling the cybercrime treaty's next steps

Source: According to... Global Initiative Against Transnational Organized Crime, September 2026

Link: <https://globalinitiative.net/wp-content/uploads/2026/09/Ian-Tennant-and-Helena-Yixin-Huang-The-present-and-future-of-the-UN-cybercrime-convention-GI-TOC-September-2026.pdf>

Fact: It states... by mid-September 2026 about 80 states, plus the European Union, had signed or joined the convention, and entry into force "could happen in 2027." The United States has taken a "wait and see" position, and human rights and privacy groups urged states not to ratify. Russia, supported by China and others, is pushing an extra protocol on terrorist and extremist uses of ICTs, but states failed to agree on rules of procedure in January 2026, and the next meeting is planned for Vienna in January 2027.

This means... even after adoption, the treaty divides the major powers. The same split, with Russia and China on one side and the United States and rights groups on the other, would shape any treaty on cyberwarfare.

Where the Major Blocs Stand

These short summaries show the starting position of the largest powers and groups. Delegates should check their own country's position, then look for the bloc closest to it.

United States

Under its March 2026 National Cyber Strategy, the United States focuses on disrupting adversaries and "imposing consequences" on those who act against it. The strategy says little about international policy or new international rules.

Source: According to... Royal United Services Institute, March 16, 2026

Link: <https://www.rusi.org/explore-our-research/publications/commentary/brief-bold-and-beautiful-reactions-us-national-cyber-strategy>

China

In July 2026 China gave the Global Mechanism a position paper saying all countries should follow the UN Charter in cyberspace and that international cyber rules should be updated "in keeping with the times." It adds "respect for digital sovereignty" to its long-held idea of cyber sovereignty and stresses each country's right to choose its own path for digital technology.

Source: According to... Ministry of Foreign Affairs of the People's Republic of China, July 23, 2026

Link:

https://www.mfa.gov.cn/eng/wjb/zzjg_663340/jks_665232/jkxw_665234/202607/t20260723_11990405.html

Russia

Russia started UN work on information security in 1998 and wants the Global Mechanism to decide everything by consensus, focus first on capacity building, and discuss "the possibility of developing legally binding agreements." It links this goal to the cybercrime convention it helped create.

Source: According to... UN Office for Disarmament Affairs (statement of the Russian Federation to the First Committee), October 27, 2025

Link: [https://docs-library.unoda.org/General_Assembly_First_Committee_-_Eightieth_session_\(2025\)/Russian_Federation_5_EN.pdf](https://docs-library.unoda.org/General_Assembly_First_Committee_-_Eightieth_session_(2025)/Russian_Federation_5_EN.pdf)

European Union

The EU calls the 11 voluntary UN norms a "central pillar" of cyber security that works alongside binding international law, not in place of it. It says international law forbids using ICTs to force another state's choices and supports a practical checklist to help states apply the norms.

Source: According to... European Union External Action Service, July 21, 2026

Link: https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-un-global-mechanism-icts-international-security-first-substantive-session-key-eu-4_en

African Union

In January 2024 the African Union adopted a Common African Position, agreed by all 55 members, which says "any unauthorized access by a State into the ICT infrastructure located on the territory of a foreign State is unlawful." It also says a cyber operation against critical infrastructure "may be considered as amounting to a use of force."

Source: According to... EJIL: Talk!, Blog of the European Journal of International Law, February 5, 2024

Link: <https://www.ejiltalk.org/the-common-african-position-on-the-application-of-international-law-in-cyberspace-reflections-on-a-collaborative-lawmaking-process/>

Pacific Small Island States

Speaking at the Global Mechanism and aligning with the Pacific Islands Forum, Micronesia reaffirmed that international law applies in cyberspace and supported the voluntary norms. It warned that small island developing states with limited technical capacity are especially exposed, called for capacity building based on each country's needs, and said the UN "must remain the principal forum for inclusive dialogue."

Source: According to... Permanent Mission of the Federated States of Micronesia to the United Nations, July 20, 2026

Link: <https://unmission.fm/wp-content/uploads/2026/07/Global-Mechanism-on-ICT.pdf>

HMDC Forensics, Harvard MUN Online, December 2026