

HMDC Presents... LEGAL: Full Report

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.

TABLE OF CONTENTS

- TABLE OF CONTENTS

- PART 1, THE TOPIC
 - The Harms
 - Council on Foreign Relations, Cyber Operations Tracker, Last Accessed October 2026
 - CSIS Significant Cyber Incidents, Last Accessed October 2026 (Kyivstar)
 - CSIS Significant Cyber Incidents, Last Accessed October 2026 (Energy Grids)
 - UK Government (GOV.UK), May 10, 2022
 - UK National Audit Office, October 27, 2017
 - U.S. Department of Justice, October 19, 2020
 - IMF Blog, April 9, 2024
 - CISA Joint Advisory AA24-038A, February 7, 2024
 - CSIS Significant Cyber Incidents, Last Accessed October 2026 (Costa Rica and Albania)
 - ICRC Position Paper, November 28, 2019
 - Associated Press, March 24, 2026
 - Associated Press, April 8, 2026
 - NPR, August 12, 2026
 - CSIS Analysis, August 6, 2026
 - Solution 1: Clarifying How Existing International Law Applies
 - UNIDIR Event Page, July 16, 2026
 - UNIDIR Publication, July 13, 2026
 - ICRC Cyber Warfare Page, Last Accessed October 2026
 - Lieber Institute, West Point, January 9, 2026
 - Solution 2: Negotiating New Binding Treaties
 - Chatham House, October 31, 2025
 - Chatham House, February 23, 2024
 - United Nations in Egypt, October 25, 2025
 - Solution 3: Holding States and Individuals Accountable
 - Chatham House, March 25, 2026
 - Chatham House, January 26, 2026
 - American Society of International Law, January 13, 2026
 - Chatham House, May 23, 2024
 - Royal United Services Institute, March 16, 2026
 - Solution 4: Building Capacity and Resilience
 - UNIDIR News, July 13, 2026
 - ITU Global Cybersecurity Index, Last Accessed October 2026
 - Chatham House, November 27, 2024
 - Lesser Solutions
 - Chatham House, October 18, 2024
 - Chatham House, June 3, 2026

- PART 2, THE UNITED NATIONS RECORD
 - UN Resolutions and Major Instruments
 - UNODA ICT Security Page, Last Accessed October 2026
 - UNODA GGE Page, Last Accessed October 2026
 - UNODA OEWG Page, Last Accessed October 2026
 - UNIDIR Analysis, April 8, 2026
 - UNIDIR Event Page, July 21, 2026
 - UNIDIR Commentary, June 24, 2026
 - UNODC Ad Hoc Committee Page, Last Accessed October 2026
 - UNODC Convention Page, Last Accessed October 2026
 - UN Press Release GA/12671, Last Accessed October 2026
 - UNIDIR Compendium, July 20, 2026
 - UNIDIR Publication, September 18, 2026
 - UN General Assembly Resolution A/RES/80/16, December 1, 2025
 - UN Geneva, November 8, 2024
 - Permanent Mission of Australia to the UN, July 22, 2026
 - Government of Canada, July 16, 2026
 - Global Initiative Against Transnational Organized Crime, September 2026
 - Where the Major Blocs Stand
 - United States
 - China
 - Russia
 - European Union
 - African Union
 - Pacific Small Island States
- PART 3, INTERNATIONAL EFFORTS
 - Carnegie Endowment for International Peace, July 29, 2025
 - European Union External Action Service, July 21, 2026
 - GOV.UK, July 13, 2026
 - Belfer Center, Harvard Kennedy School, September 2022
 - NATO Cyber Defence Page, July 30, 2024
 - Council of the EU Declaration, May 10, 2022
 - Council of Europe Budapest Convention, Last Accessed October 2026
 - African Union Treaty Page, Last Accessed October 2026
 - NATO CCDCOE Tallinn Manual Page, Last Accessed October 2026
 - Paris Call Website, Last Accessed October 2026
 - GOV.UK Pall Mall Process, April 4, 2025
 - Global Forum on Cyber Expertise, Last Accessed October 2026
 - ASEAN Secretariat, April 2026
 - Cyber Security Agency of Singapore, October 24, 2025
 - Cybersecurity Tech Accord, November 8, 2024
 - Oxford Process, Last Accessed October 2026
 - Protect.ngo (formerly CyberPeace Institute), Last Accessed October 2026
 - World Economic Forum, January 13, 2025
 - CSIS Significant Cyber Incidents, Last Accessed October 2026 (Telecoms and Crypto)
- KEY VOCABULARY
- DISCUSSION QUESTIONS

PART 1, THE TOPIC

The Legal Committee (the Sixth Committee of the General Assembly) is the main UN forum for legal questions. For this committee, "cyberwarfare case studies" means looking at real cyber operations by states, or by groups working for states, and asking what the law says about them. The central question is whether existing international law, including the UN Charter and international humanitarian law (the law of war), already covers these operations, or whether the world needs new and clearer legal rules.

The Harms

Cyber operations are no longer rare. They hit power grids, hospitals, telephone networks and banks, and the harm often spreads far beyond the country that was the target. The entries below show who is hurt, how many people are affected, and how serious the damage can be.

Council on Foreign Relations, Cyber Operations Tracker, Last Accessed October 2026

Tagline: Counting state-sponsored cyber operations

Source: According to... Council on Foreign Relations, Last Accessed: October 2026

Link: <https://www.cfr.org/cyber-operations/>

Fact: It states... the tracker records publicly known cyber operations sponsored by states since 2005. Thirty-four countries are suspected of sponsoring operations, and four of them (China, Russia, Iran and North Korea) account for 77 percent of the suspected operations. In 2019 alone it counted seventy-six operations, most of them spying.

This means... cyber operations are a regular tool of state power, not a rare event. A legal resolution must work for dozens of states, including the few states responsible for most operations.

CSIS Significant Cyber Incidents, Last Accessed October 2026 (Kyivstar)

Tagline: Cutting phone service for millions

Source: According to... Center for Strategic and International Studies, Last Accessed: October 2026

Link: <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>

Fact: It states... in December 2023 Russian hackers attacked Kyivstar, Ukraine's largest mobile phone company, and disabled service for its 24 million customers.

This means... one cyber operation during a war can cut off ordinary civilians from calls, emergency services and family. Delegates must decide whether attacks like this count as an "attack" on a civilian object under the law of war.

CSIS Significant Cyber Incidents, Last Accessed October 2026 (Energy Grids)

Tagline: Targeting European energy systems

Source: According to... Center for Strategic and International Studies, Last Accessed: October 2026

Link: <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>

Fact: It states... in November 2023 Russian hackers struck twenty-two Danish power companies, which the list calls Denmark's largest cyberattack on record. Between December 2025 and January 2026, a coordinated attack hit about 30 sites connected to Poland's energy grid and disrupted control systems, though it caused no widespread blackout. Researchers linked it to a Russia-aligned group.

This means... energy systems in countries that are not at war are also being targeted. The committee must consider what the law says about cyber operations that happen in peacetime, below the level of armed conflict.

UK Government (GOV.UK), May 10, 2022

Tagline: Damaging satellite internet across Europe

Source: According to... GOV.UK, May 10, 2022

Link: <https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion>

Fact: It states... on February 24, 2022, about an hour before Russia's full invasion of Ukraine, a cyberattack hit the satellite company Viasat. Several thousand Ukrainian customers lost internet, wind farms in central Europe were disrupted, and Viasat said tens of thousands of user terminals were damaged beyond repair. The United Kingdom, the European Union, the United States and allies publicly blamed Russia on May 10, 2022.

This means... a cyber operation aimed at a military target can spill over and harm civilians in many other countries. This case is central to debates on distinction (separating military from civilian targets) and proportionality.

UK National Audit Office, October 27, 2017

Tagline: Disrupting hospitals and patient care

Source: According to... UK National Audit Office, October 27, 2017

Link: <https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/>

Fact: It states... the WannaCry attack, released worldwide on May 12, 2017, affected at least 81 of 236 hospital trusts in England (about 34 percent). An estimated 19,000 or more medical appointments were cancelled.

This means... cyberattacks can directly harm patients. Medical services have special protection under the law of war, so delegates can argue for an explicit rule protecting health care from cyber operations at all times.

U.S. Department of Justice, October 19, 2020

Tagline: Charging officers for destructive malware

Source: According to... U.S. Department of Justice, October 19, 2020

Link: <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>

Fact: It states... six Russian military intelligence (GRU) officers were charged for a series of attacks: blackouts in Ukraine's power grid in 2015 and 2016, the NotPetya malware in June 2017, and an attack on the 2018 Winter Olympics opening ceremony. NotPetya caused nearly \$1 billion in losses to just three victims, and a hospital system lost its critical computer systems for about a week.

This means... the NotPetya case shows that one operation can spread worldwide and cause huge economic and medical harm. It also shows one accountability tool: charging individual officers, even when they are unlikely to ever face trial.

IMF Blog, April 9, 2024

Tagline: Measuring rising financial losses

Source: According to... International Monetary Fund, April 9, 2024

Link: <https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability>

Fact: It states... cyberattacks have more than doubled since the COVID-19 pandemic, and the size of extreme losses from cyber incidents has more than quadrupled since 2017, to \$2.5 billion. Only about half of central banks and financial supervisors surveyed had a cybersecurity strategy or rules for the financial sector, with the largest gaps in developing economies.

This means... the harm is economic as well as physical, and poorer countries are less protected. Any solution that ignores capacity gaps will leave developing countries most exposed.

CISA Joint Advisory AA24-038A, February 7, 2024

Tagline: Prepositioning inside critical infrastructure

Source: According to... U.S. Cybersecurity and Infrastructure Security Agency, February 7, 2024

Link: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>

Fact: It states... a Chinese state-sponsored group called Volt Typhoon hid inside networks for communications, energy, transport and water systems, in some cases for years. The agencies, joined by partners in Australia, Canada, the United Kingdom and New Zealand, judged with high confidence that the goal was to be ready to disrupt or destroy these systems in a future crisis or conflict, not ordinary spying.

This means... some cyber operations prepare for future attacks during peacetime. The committee must ask whether hiding inside another country's water or power system already breaks international law (for example, the rule of sovereignty or non-intervention).

CSIS Significant Cyber Incidents, Last Accessed October 2026 (Costa Rica and Albania)

Tagline: Paralyzing entire national governments

Source: According to... Center for Strategic and International Studies, Last Accessed: October 2026

Link: <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>

Fact: It states... in April 2022 hackers attacked Costa Rica's Ministry of Finance, crippling tax collection and export systems, and the new president declared a national emergency; the group demanded \$20 million. In July and September 2022, Iranian actors shut down Albanian government websites, destroyed data with ransomware, and forced Albania to shut down its border-tracking system.

This means... small and medium countries can have their whole government paralyzed. These cases raise the question of when a state is responsible for criminal or proxy groups, and what help other states should give.

ICRC Position Paper, November 28, 2019

Tagline: Warning about civilian human cost

Source: According to... International Committee of the Red Cross, November 28, 2019

Link: <https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts>

Fact: It states... cyber operations are already part of armed conflicts, but only a few states have publicly admitted using them. Many states are building military cyber capabilities, and recent operations have disrupted civilian infrastructure and may cause human harm.

This means... the ICRC, the guardian of the law of war, believes the risk to civilians is real and growing. Its position gives delegates a neutral, respected basis for arguing that international humanitarian law applies to cyber operations.

Associated Press, March 24, 2026

Tagline: Attacking heat and power in winter

Source: According to... Associated Press, March 24, 2026

Link: <https://wtop.com/russia-ukraine-war-news/2026/03/poland-faced-a-surge-in-cyberattacks-in-2025-including-a-major-assault-on-the-energy-sector/>

Fact: It states... Poland faced about 270,000 cyberattacks in 2025, around two and a half times more than the year before. On December 29, 2025, coordinated attacks hit a heat and power plant that serves nearly 500,000 customers, along with several wind and solar farms. Electricity was not cut. The attack aimed to destroy, not to make money, and the report calls it likely unprecedented among NATO and EU members. Experts linked the tools to groups tied to Russian intelligence.

This means... a peacetime attack on heating in winter could hurt hundreds of thousands of civilians in a country that is not at war. Delegates must decide whether such an attack breaks the rule of sovereignty, the rule of non-intervention, or both.

Associated Press, April 8, 2026

Tagline: Threatening ports, power and water

Source: According to... Associated Press, April 8, 2026

Link: <https://pbs.org/newshour/world/shaky-ceasefire-unlikely-to-stop-cyberattacks-from-iran-linked-hackers-for-long>

Fact: It states... during the 2026 war between Iran, the United States and Israel, U.S. authorities warned that hackers supported by Iran had gained access to control devices used in ports, power plants and water plants. A pro-Iran group called Handala claimed it disrupted a U.S. medical equipment company, and pro-Iran hackers targeted data centers and industrial sites in Israel, Saudi Arabia and Kuwait. Handala said a two-week ceasefire would not end its attacks. Experts described the attacks so far as high in number but low in impact.

This means... cyber operations do not stop when the guns stop. The committee must ask whether "hactivist" groups that support a state at war can be legally linked to that state, and whether a ceasefire should also cover cyberspace.

NPR, August 12, 2026

Tagline: Disrupting drinking water in small towns

Source: According to... NPR, August 12, 2026

Link: <https://www.opb.org/article/2026/08/12/cyberattacks-on-the-u-s-water-sector-are-exposing-vulnerabilities-during-iran-war/>

Fact: It states... between about July 26 and July 28, 2026, attackers targeted water and wastewater systems in at least seven U.S. states, according to the FBI. In Braham, Minnesota, a treatment plant pump failed and about 1,700 residents were asked to save water, and more than 30 Minnesota water systems were targeted. The attackers used devices left open to the internet with factory-set passwords that were never changed. The U.S. government had not officially named who was responsible, though officials suspected Iran.

This means... small towns with weak defences are easy targets, and the harm reaches families directly. The case also shows why attribution matters: without an official finding, the legal tools of state responsibility and countermeasures are hard to use.

CSIS Analysis, August 6, 2026

Tagline: Linking hacking to battlefield strikes

Source: According to... Center for Strategic and International Studies, August 6, 2026

Link: <https://www.csis.org/analysis/how-tehrans-use-cyber-operations-us-iran-conflict-has-evolved>

Fact: It states... Iran's cyber forces have been "regeared" to support its war effort. Hackers targeted defence companies, senior U.S. and Israeli officials, U.S. water systems, and security cameras in several countries, which were used to aim weapons and check damage. Hacking a global telephone signalling system reportedly helped locate U.S. troops and directly informed strikes that caused injuries. Artificial intelligence increased the speed and reach of these operations.

This means... in modern war, cyber operations are part of the fighting itself and can lead to real injuries. This supports the argument that the law of war, including distinction and proportionality, must clearly govern cyber operations, and it raises the question of whether hacking private civilian cameras to aim weapons is lawful.

Solution 1: Clarifying How Existing International Law Applies

This solution says the world does not need a new treaty. Instead, states should agree on how the rules they already have (the UN Charter, state responsibility and international humanitarian law) apply in cyberspace, often by publishing "national positions."

UNIDIR Event Page, July 16, 2026

Tagline: Publishing national legal positions

Source: According to... United Nations Institute for Disarmament Research, July 16, 2026

Link: <https://unidir.org/event/advancing-common-understandings-on-the-application-of-international-law-in-cyberspace-pre-launch-of-mauritius-national-position/>

Fact: It states... 36 states and two regional organizations have published positions on how international law applies in cyberspace. Mauritius was preparing to become the first African Union member to publish one after the 2024 Common African Position.

This means... a resolution could encourage every state to publish a national position and offer help to those that lack legal experts.

UNIDIR Publication, July 13, 2026

Tagline: Exposing disagreement over key definitions

Source: According to... United Nations Institute for Disarmament Research, July 13, 2026

Link: <https://unidir.org/publication/international-humanitarian-law-and-cyber-operations-consequences-of-divergent-national-interpretations-of-attack-and-data/>

Fact: It states... after more than ten years of UN talks, states still do not share an understanding of how the law of war applies to cyber operations. A "restrictive" group counts only operations that cause physical damage as "attacks" and usually does not protect data. An "expansive" group counts operations that cause a loss of functionality as attacks and protects essential civilian data. The report warns that this gap could weaken protection for civilians.

This means... two definitions decide almost every case study: what is an "attack," and is data an "object" that cannot be targeted. A precise resolution could aim at these two questions.

ICRC Cyber Warfare Page, Last Accessed October 2026

Tagline: Applying humanitarian law to all weapons

Source: According to... International Committee of the Red Cross, Last Accessed: October 2026

Link: <https://www.icrc.org/en/war-and-law/conduct-hostilities/cyber-warfare>

Fact: It states... international humanitarian law is the main law governing cyber operations in war, and its rules apply to all weapons, including new ones. Core protections, such as the ban on targeting civilians, the ban on indiscriminate or disproportionate attacks, and the duty to protect medical services, also apply in cyberspace. Open questions remain about civilian data and about operations that disrupt systems without physical damage.

This means... delegates who prefer clarifying existing law can rely on the ICRC. Delegates who want a new treaty can point to the open questions the ICRC itself admits.

Lieber Institute, West Point, January 9, 2026

Tagline: Affirming the law but avoiding detail

Source: According to... Lieber Institute for Law and Warfare, United States Military Academy at West Point, January 9, 2026

Link: <https://lieber.westpoint.edu/law-of-cyber-operations/>

Fact: It states... during 2025, states kept saying that international humanitarian law applies to cyber operations in war, but they avoided explaining how it applies. They did not agree whether a loss of functionality, corrupted data or blocked access counts as an "attack." The 2025 UN working group report repeated that international law applies, but warned against using the law of war in a way that could make conflict seem legitimate. The author expects states in 2026 to keep affirming the law "in principle while resisting its elaboration in cyber contexts."

This means... the clarification solution faces a real obstacle: many states prefer to keep the rules vague so they keep their freedom to act. Delegates who want clarity may need to offer something in return, such as help with legal capacity.

Weighing this solution. Advantages: National positions build agreement step by step without a long treaty negotiation. Existing law already offers strong protections that states have accepted. Disadvantages: 36 states is a small share of the 193 UN members, so most states have not yet said what they believe the law requires. Clarifying existing law is slow, full agreement is unlikely, and expert reviews of 2025 found that states avoided explaining how the law of war applies in cyberspace.

Solution 2: Negotiating New Binding Treaties

This solution says voluntary norms are not enough and the world needs legally binding rules, like a treaty. The UN has already adopted one cyber treaty, on crime, which shows both what is possible and what is difficult.

Chatham House, October 31, 2025

Tagline: Weighing the new cybercrime treaty

Source: According to... Chatham House, October 31, 2025

Link: <https://www.chathamhouse.org/2025/10/au-can-help-african-countries-adopt-un-cybercrime-convention-challenges-are-significant>

Fact: It states... the UN Convention against Cybercrime opened for signature in Hanoi on October 25, 2025, and needs 40 ratifications to enter into force; 21 African countries had already signed. African states lose over \$4 billion a year to cybercrime. However, national cybercrime laws have often been used to restrict free expression, and the African Union's own cyber treaty (Malabo) has been ratified by only 16 of 55 members.

This means... a cyberwarfare treaty would face the same tests: will enough states join, and will it protect rights? The Malabo record warns that signing is not the same as acting.

Chatham House, February 23, 2024

Tagline: Showing slow treaty ratification

Source: According to... Chatham House, February 23, 2024

Link: <https://www.chathamhouse.org/2024/02/au-took-important-action-cybersecurity-its-2024-summit-more-needed>

Fact: It states... the African Union's Malabo Convention was adopted in 2014 but only entered into force on June 8, 2023, nine years later. Large states such as Egypt, Algeria, Nigeria, South Africa, Kenya, Morocco and Ethiopia had not ratified it. At the same 2024 summit, the African Union agreed a Common African Position on how international law applies in cyberspace.

This means... a quicker non-binding step (a common position) was achieved in the same year that the binding treaty was still stalled. Delegates can use this to argue for a two-track approach.

United Nations in Egypt, October 25, 2025

Tagline: Signing the first global cyber treaty

Source: According to... United Nations in Egypt, October 25, 2025

Link: <https://egypt.un.org/en/303974-un-convention-against-cybercrime-opens-signature-hanoi-vietnam>

Fact: It states... 65 states signed the UN Convention against Cybercrime on the first day it opened for signature in Hanoi, Viet Nam. Secretary-General António Guterres called it "a powerful, legally binding instrument." It is the first global framework for collecting and sharing electronic evidence of serious crimes, and it creates a network that works 24 hours a day, 7 days a week for fast cooperation between states. It enters into force 90 days after the fortieth state ratifies it.

This means... the UN can produce a binding cyber treaty that many states sign quickly. Delegates who want a treaty on state cyber operations can point to this success, while others can note that this treaty covers crime and not attacks by states.

Weighing this solution. Advantages: A binding treaty creates shared rules and channels for cooperation. Disadvantages: Treaties can be slow to ratify, and they can be misused to limit human rights. Binding treaties can take close to a decade to take effect.

Solution 3: Holding States and Individuals Accountable

This solution focuses on consequences: naming the state responsible (attribution), sanctions, legal countermeasures, and criminal trials for individuals. The challenge is that cyber operations are often hidden or carried out by "proxies" (groups that are not officially part of a government).

Chatham House, March 25, 2026

Tagline: Closing gaps for cyber proxies

Source: According to... Chatham House, March 25, 2026

Link: <https://www.chathamhouse.org/2026/03/holding-state-sponsored-hackers-and-other-cyber-proxies-account>

Fact: It states... Russia uses criminal groups, "hacktivists" and private companies as cyber proxies, which gives it deniability and makes attribution difficult. Because the legal bar for linking non-state conduct to a state is high, Russia often avoids responsibility. Responses so far have won tactical victories but have not weakened these actors strategically, and they often rebuild quickly. The paper recommends combining prosecutions with coordinated sanctions on hosting companies, payment processors and cryptocurrency exchanges.

This means... the law of state responsibility may be too narrow for cyber proxies. The Legal Committee could debate whether the test for state responsibility needs clarifying.

Chatham House, January 26, 2026

Tagline: Prosecuting cyber-enabled international crimes

Source: According to... Chatham House, January 26, 2026

Link: <https://www.chathamhouse.org/2026/01/securing-justice-cyber-enabled-international-crimes>

Fact: It states... cyber means can be used to commit war crimes, crimes against humanity, genocide and aggression, and international criminal law is "technology-neutral." In December 2025 the International Criminal Court's Prosecutor published a policy promising to investigate cyber-enabled crimes on an equal basis with traditional ones. Gaps remain: many national laws do not cover these crimes, attribution is hard, and judges and prosecutors may not be ready.

This means... delegates can call on states to update their national laws and cooperate with the ICC, a legal step that falls directly within the Sixth Committee's work.

American Society of International Law, January 13, 2026

Tagline: Applying the Rome Statute to cyberspace

Source: According to... American Society of International Law, January 13, 2026

Link: <https://www.asil.org/ILIB/icc-otp-issues-first-policy-cyber-enabled-crimes>

Fact: It states... on December 3, 2025, the Office of the Prosecutor of the International Criminal Court issued its first Policy on Cyber-Enabled Crimes. The policy says genocide, crimes against humanity, war crimes and aggression can be committed fully or partly through cyber means, and that the Rome Statute "applies fully" to conduct in cyberspace. It also promises to build skills for collecting and checking digital evidence, and it looks at how artificial intelligence may affect who is responsible.

This means... an international court now says that some cyber operations can be prosecuted as the most serious international crimes. Delegates can ask states to match this in their national laws so that cyber war crimes do not escape punishment.

Chatham House, May 23, 2024

Tagline: Explaining legal countermeasures in cyberspace

Source: According to... Chatham House, May 23, 2024

Link: <https://www.chathamhouse.org/2024/05/countermeasures-international-law-and-their-role-cyberspace>

Fact: It states... countermeasures (actions that would normally be unlawful but are allowed in response to another state's violation) apply in cyberspace. Existing rules are flexible enough for fast and secret responses. However, it is unsettled whether third states that were not harmed may take "collective" countermeasures, though support for them is growing.

This means... a key legal debate for this committee is whether allies can lawfully respond together on behalf of a small state that was attacked.

Royal United Services Institute, March 16, 2026

Tagline: Shifting toward offensive cyber responses

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>

Fact: It states... the United States released a new National Cyber Strategy in early March 2026. Its first pillar, "shape adversary behaviour," focuses on disrupting adversaries and "imposing consequences on those who do act against us," and it proposes incentives for private companies to identify and disrupt adversary networks. RUSI experts noted that the strategy says little about international policy and names no specific adversary, and that giving private companies an offensive role raises risks that need careful study.

This means... the world's leading cyber power is leaning toward punishment and disruption rather than new international rules. Delegates can debate whether letting private companies "hack back" fits the law of state responsibility, since a state can be responsible for what private actors do on its behalf.

Weighing this solution. Advantages: Targeting individuals and supporting infrastructure works even without full proof against a state. Individual criminal responsibility can deter people who carry out operations. A harmed state can lawfully respond to stop a breach. Disadvantages: Action is fragmented and proxies regroup. Evidence is difficult to collect and authenticate. Loosening the conditions risks escalation, and the law on collective countermeasures is uncertain. Giving private companies a role in disrupting adversaries could blur the line between lawful responses and unlawful attacks.

Solution 4: Building Capacity and Resilience

This solution says the most effective protection is helping every country defend its own systems. It focuses on training, national strategies and basic security, especially for developing countries.

UNIDIR News, July 13, 2026

Tagline: Turning norms into national practice

Source: According to... United Nations Institute for Disarmament Research, July 13, 2026

Link: <https://unidir.org/unidir-and-thailand-advance-national-implementation-of-un-cyber-norms/>

Fact: It states... UNIDIR worked with Thailand's security and foreign affairs agencies in July 2026 to turn UN cyber norms into national policy, using briefings and practice exercises. A May 2025 exercise simulating a major incident led to a national roadmap. Similar training took place in Indonesia, Laos, Malaysia, Pakistan and the Philippines, following the principle that support should be requested by the country and fit its needs.

This means... a resolution can link legal norms to concrete training, rather than leaving them on paper.

ITU Global Cybersecurity Index, Last Accessed October 2026

Tagline: Ranking national cybersecurity commitments

Source: According to... International Telecommunication Union, Last Accessed: October 2026

Link: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>

Fact: It states... the 2024 Global Cybersecurity Index (fifth edition) measures countries across five pillars: legal, technical, organizational, capacity development and cooperation. It was built from a review of over 30,000 web pages, more than 1,000 documents and exchanges with member states.

This means... "legal measures" are one pillar, so the Legal Committee can recommend that weaker states receive help writing cyber laws.

Chatham House, November 27, 2024

Tagline: Rejecting cyber doomsday warnings

Source: According to... Chatham House, November 27, 2024

Link: <https://www.chathamhouse.org/2024/11/why-cyber-doomsday-warnings-do-more-harm-good>

Fact: It states... warnings of a "cyber doomsday" create fear and distract from more common threats such as ransomware, spying and weak supply chains. Predicted collapses have not happened, and the war in Ukraine shows cyber operations are disruptive but do not replace conventional military power. The author argues for widespread basic security and resilience.

This means... delegates should judge the case studies by their real effects, and resilience may help more than dramatic new rules.

Weighing this solution. Advantages: Practical help makes the UN norms real inside each country. The index shows which countries need help and in which area. Resilience reduces harm from every kind of operation, whoever is responsible. Disadvantages: It is slow, country by country, and depends on donor funding.

Lesser Solutions

These ideas are narrower but may appear in draft resolutions.

Chatham House, October 18, 2024

Tagline: Regulating the commercial hacking market

Source: According to... Chatham House, October 18, 2024

Link: <https://www.chathamhouse.org/2024/10/principles-state-approaches-commercial-cyber-intrusion-capabilities>

Fact: It states... hacking tools are bought and sold by states, companies and criminals, which has greatly expanded who can use them. Many states buy them rather than build them, and often use them in ways that conflict with human rights law. The paper proposes eight principles, including separating permitted security testing from unpermitted intrusion and not letting private firms hack on a state's behalf.

This means... controlling the market for hacking tools is a lesser but practical solution that reduces how many actors can carry out operations.

Chatham House, June 3, 2026

Tagline: Preparing for AI cyber threats

Source: According to... Chatham House, June 3, 2026

Link: <https://www.chathamhouse.org/2026/06/face-growing-ai-cyber-threats-do-middle-powers-have-agency>

Fact: It states... advanced artificial intelligence models can find and fix network weaknesses far faster than humans, but the same ability could make cyberattacks much more powerful. Access to these models is limited mostly to a few countries and firms. The author recommends that middle powers coordinate, share information with companies, and prepare emergency backchannels.

This means... new technology may make today's legal gaps more dangerous, so delegates can propose that the UN study how existing law applies to AI-assisted cyber operations.

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>

PART 3, INTERNATIONAL EFFORTS

Outside the UN, many regional organizations, alliances, treaties and NGOs work on cyber conflict. Some create binding law for their members, some set voluntary principles, and some help victims directly.

Carnegie Endowment for International Peace, July 29, 2025

Tagline: Judging twenty years of cyber diplomacy

Source: According to... Carnegie Endowment for International Peace, July 29, 2025

Link: <https://carnegieendowment.org/posts/2025/07/un-cyber-diplomacy-oewg-successes-shortcomings>

Fact: It states... the final session of the 2021-2025 working group agreed on a permanent UN body, the Global Mechanism, which starts work in 2026 with a review proposed for 2031. The author calls capacity building the "star performer" of cyber diplomacy, but describes the twenty-year record as "arguably unimpressive." The eleven norms agreed in 2015 are voluntary, carry no real accountability, and the ones that forbid certain actions are often ignored. The author recommends more regional and small-group cooperation and pressure on states that break the norms.

This means... a leading think tank doubts that voluntary norms alone change state behaviour. Delegates who favour binding law can quote this, while others can argue that capacity building is the part that is working.

European Union External Action Service, July 21, 2026

Tagline: Testing norms at the Global Mechanism

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

Fact: It states... at the first working session of the Global Mechanism (July 20-24, 2026), the EU called the 11 voluntary UN norms a "central pillar" of security in cyberspace. It said voluntary norms work alongside binding international law, and that international law forbids using ICTs to force another state's choices (coercive interference). It said the norms tell states not to use tools such as ransomware to disrupt critical infrastructure, and it supported a draft checklist to help states put the norms into practice.

This means... the EU, a major regional bloc, treats the norms and binding law as partners, not rivals. Delegates can propose that the Sixth Committee support the norms checklist and link it to clear legal rules.

GOV.UK, July 13, 2026

Tagline: Sanctioning hackers through joint action

Source: According to... GOV.UK, July 13, 2026

Link: <https://www.gov.uk/government/news/uk-and-eu-strike-russian-cyber-networks-with-new-sanctions>

Fact: It states... in what it calls their first joint cyber sanctions package, the United Kingdom and the European Union acted together against Russian cyber and hybrid operations, with the UK sanctioning 24 people and organizations. The UK and EU member states blamed Russia's FSB Centre 16 for the failed attack on Poland's energy grid, which could have left 500,000 people without electricity in winter. Foreign Secretary Yvette Cooper said the action shows Russia cannot hide behind proxy groups.

This means... states are joining forces to name and punish those responsible, even when proxies are used. Delegates can debate whether such joint sanctions are lawful collective countermeasures and whether the UN should set rules for them.

Belfer Center, Harvard Kennedy School, September 2022

Tagline: Ranking the world's cyber powers

Source: According to... Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2022

Link: <https://www.belfercenter.org/publication/national-cyber-power-index-2022>

Fact: It states... the National Cyber Power Index ranks 30 countries using 29 indicators and more than 1,000 data sources. The top ten were the United States, China, Russia, the United Kingdom, Australia, the Netherlands, South Korea, Viet Nam, France and Iran. One goal it measures is how much each state takes part in shaping international cyber norms, such as joining UN expert groups and the Global Forum on Cyber Expertise. It describes the link between technology and values as a "growing fault line" in world affairs.

This means... the states with the most cyber power also try hardest to shape the rules. Smaller states that want a voice in cyber law may need to work together to balance them.

NATO Cyber Defence Page, July 30, 2024

Tagline: Treating cyberattacks as collective defence

Source: According to... North Atlantic Treaty Organization, July 30, 2024

Link: https://www.nato.int/cps/en/natohq/topics_78170.htm

Fact: It states... NATO adopted its first cyber defence policy in 2008 after the 2007 attacks on Estonia. In 2014 it agreed a cyberattack could lead to invoking Article 5 (collective defence), and in 2016 it recognized cyberspace as a domain of operations. Its 2021 policy says significant cumulative malicious cyber activity might, case by case, count as an armed attack. In 2024 it agreed to create an Integrated Cyber Defence Centre.

This means... a major alliance treats serious cyberattacks like armed attacks. This raises the legal question of when a cyber operation reaches the "armed attack" level that allows self-defence under Article 51 of the UN Charter.

Council of the EU Declaration, May 10, 2022

Tagline: Condemning attacks through joint statements

Source: According to... Council of the European Union, May 10, 2022

Link: <https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/>

Fact: It states... the EU and its member states condemned Russia's cyberattack on the KA-SAT satellite network, which took place one hour before the February 24, 2022 invasion and disrupted Ukrainian authorities, businesses and users as well as several EU states. The EU called it a breach of expectations for responsible state behaviour and promised more support for Ukraine's cyber resilience.

This means... joint public attribution is a common international response. It names the responsible state but does not by itself impose a legal penalty.

Council of Europe Budapest Convention, Last Accessed October 2026

Tagline: Expanding the oldest cybercrime treaty

Source: According to... Council of Europe, Last Accessed: October 2026

Link: <https://www.coe.int/en/web/cybercrime/the-budapest-convention>

Fact: It states... the Budapest Convention on Cybercrime has 83 parties, with 14 more countries having signed or been invited to join, and any state may join. It has two additional protocols, including one on enhanced cooperation and sharing electronic evidence. Non-parties use it as a model law.

This means... a regional treaty can become global over time. Delegates can compare it to the new UN convention when debating whether binding cyber rules spread widely.

African Union Treaty Page, Last Accessed October 2026

Tagline: Adopting an African cyber treaty

Source: According to... African Union, Last Accessed: October 2026

Link: <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

Fact: It states... the African Union Convention on Cyber Security and Personal Data Protection was adopted on June 27, 2014.

This means... Africa has its own legal framework, which, together with the 2024 Common African Position, shows African states shaping cyber law rather than only following others.

NATO CCDCOE Tallinn Manual Page, Last Accessed October 2026

Tagline: Explaining law for cyber operations

Source: According to... NATO Cooperative Cyber Defence Centre of Excellence, Last Accessed: October 2026

Link: <https://ccdcOE.org/research/tallinn-manual/>

Fact: It states... the first Tallinn Manual (2013) explained how international law applies to the most severe cyber operations, such as use of force and armed conflict. Tallinn Manual 2.0 (2017) covered everyday incidents below those thresholds. A five-year revision, Tallinn Manual 3.0, began in 2021.

This means... the Tallinn Manual is an expert study, not a treaty, but delegates often cite it. Some states see it as Western-led, which is a point other delegates may raise.

Paris Call Website, Last Accessed October 2026

Tagline: Gathering states and companies together

Source: According to... Paris Call for Trust and Security in Cyberspace, Last Accessed: October 2026

Link: <https://pariscall.international/en/>

Fact: It states... French President Emmanuel Macron launched the Paris Call on November 12, 2018, at the Internet Governance Forum at UNESCO. It rests on nine shared principles and is supported by governments, civil society groups and companies, including the European Union and the United States.

This means... voluntary declarations can include companies, which own most of the internet. The disadvantage is that they create no binding duties.

GOV.UK Pall Mall Process, April 4, 2025

Tagline: Limiting commercial hacking tools

Source: According to... GOV.UK, April 4, 2025

Link: <https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states>

Fact: It states... the Pall Mall Process, led by the United Kingdom and France, launched a voluntary code of practice in Paris in April 2025 for how states develop, buy and use commercial cyber intrusion tools. It rests on four pillars: accountability, precision, oversight and transparency. Supporters include South Korea, Finland, Romania, the United States, Latvia and, from October 2025, Belgium as a signatory.

This means... states are starting to set rules for the market in hacking tools, which feeds cyber operations. The code is voluntary, so it depends on willing states.

Global Forum on Cyber Expertise, Last Accessed October 2026

Tagline: Coordinating cyber capacity building worldwide

Source: According to... Global Forum on Cyber Expertise, Last Accessed: October 2026

Link: <https://thegfce.org/>

Fact: It states... the GFCE is a community of over 260 members and partners, including governments, international organizations, companies and universities, and describes itself as the platform for international cooperation on cyber capacity. It marked its tenth anniversary in 2025.

This means... a resolution calling for capacity building can point to an existing network rather than creating a new body.

ASEAN Secretariat, April 2026

Tagline: Planning regional cyber cooperation to 2030

Source: According to... ASEAN Secretariat, April 2026

Link: https://asean.org/wp-content/uploads/2026/07/ASEAN-Cybersecurity-Cooperation-Strategy_08072026_FIN.pdf

Fact: It states... the ASEAN Cybersecurity Cooperation Strategy 2026-2030 commits Southeast Asian states to the UN Charter, sovereignty, non-intervention and the peaceful settlement of disputes. ASEAN follows the 11 voluntary UN norms, finished a checklist for putting them into practice in September 2024, and opened a facility for its Regional Computer Emergency Response Team in October 2024. Its two regional training centres had trained more than 4,700 officials by 2025, and it plans courses in international law and digital evidence.

This means... regional groups can turn UN norms into practical plans faster than the whole UN can. A resolution can invite regional bodies, such as ASEAN and the African Union, to report on how they apply international law in cyberspace.

Cyber Security Agency of Singapore, October 24, 2025

Tagline: Uniting countries against ransomware

Source: According to... Cyber Security Agency of Singapore, October 24, 2025

Link: <https://www.csa.gov.sg/news-events/press-releases/singapore-hosted-the-5th-counter-ransomware-initiative-summit/>

Fact: It states... the fifth International Counter Ransomware Initiative summit, held in Singapore, brought together nearly 150 representatives from 60 countries, international organizations and companies. The initiative has 74 member countries and international organizations. Members agreed to share more information, improve communication between companies and governments, and build capacity, and 67 members endorsed a guide to protect supply chains from ransomware.

This means... a coalition outside the UN can act quickly against one specific harm. Its disadvantage is that only willing states join, so states accused of hosting ransomware groups are not part of it.

Cybersecurity Tech Accord, November 8, 2024

Tagline: Committing companies to cyber peace

Source: According to... Cybersecurity Tech Accord, November 8, 2024

Link: <https://cybertechaccord.org/>

Fact: It states... the Tech Accord, a group of technology companies, passed 160 signatories in November 2024. It publishes statements on topics such as AI, connected devices and "cyber mercenaries."

This means... private companies are active in cyber peace efforts. Delegates must decide what role companies should have in a UN legal process designed for states.

Oxford Process, Last Accessed October 2026

Tagline: Clarifying protections for health care

Source: According to... University of Oxford, Institute for Ethics, Law and Armed Conflict, Last Accessed: October 2026

Link: <https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/>

Fact: It states... the Oxford Process, started in May 2020 with Microsoft, brings experts together to identify rules of international law that apply to cyber operations. It has issued five statements, including on cyber operations against the health care sector, foreign election interference, information operations and ransomware.

This means... university experts have already drafted legal statements on specific harms, such as attacks on hospitals, which delegates can use as a basis for resolution language.

Protect.ngo (formerly CyberPeace Institute), Last Accessed October 2026

Tagline: Defending nonprofits from cyber harm

Source: According to... Protect.ngo, Last Accessed: October 2026

Link: <https://protect.ngo/>

Fact: It states... the Geneva-based organization, formerly called the CyberPeace Institute, exposes cyber harm, sends cyber volunteers to defend nonprofits, builds coalitions of states and donors, and holds states accountable. It also runs a tracker of cyberattacks that disrupt health care.

This means... international NGOs document harm to civilians and help victims directly, filling gaps that states have not filled.

World Economic Forum, January 13, 2025

Tagline: Linking geopolitics and cyber risk

Source: According to... World Economic Forum, January 13, 2025

Link: <https://www.weforum.org/publications/global-cybersecurity-outlook-2025/>

Fact: It states... the Global Cybersecurity Outlook 2025 describes a cyber landscape made more intense by geopolitical tensions, new technologies, supply chain dependence and more sophisticated cybercrime.

This means... cyber risk rises when tensions between states rise, so legal limits on state cyber operations are connected to wider peace and security.

CSIS Significant Cyber Incidents, Last Accessed October 2026 (Telecoms and Crypto)

Tagline: Spying on global telecom networks

Source: According to... Center for Strategic and International Studies, Last Accessed: October 2026

Link: <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>

Fact: It states... in November 2024 the Chinese group Salt Typhoon breached at least eight U.S. telecom companies and telecom providers in more than twenty other countries. In February 2025, North Korean hackers stole about \$1.5 billion in cryptocurrency from the exchange Bybit, the largest such theft on the list. In February 2026 a China-linked group breached all four major Singapore telecom providers.

This means... international efforts must deal with both spying (which international law does not clearly ban) and theft that funds states under UN sanctions. Delegates must decide which of these the committee can realistically address.

KEY VOCABULARY

1. **Attribution:** Identifying who carried out a cyber operation, especially which state is responsible.
2. **International humanitarian law (IHL):** The law of war; rules that limit how armed conflict is fought and protect civilians.
3. **Distinction:** The IHL rule that attacks may target only military objectives, never civilians or civilian objects.
4. **Proportionality:** The IHL rule that expected harm to civilians must not be excessive compared with the military advantage expected.
5. **Due diligence:** The principle that a state should not knowingly allow its territory to be used to harm other states.
6. **Sovereignty:** A state's authority over its own territory, including the computer systems inside it.
7. **Non-intervention:** The rule that a state must not force its will on another state's internal affairs, such as elections.
8. **Countermeasures:** Actions that would normally be unlawful but are allowed in response to another state's violation, to make it stop.
9. **Cyber proxy:** A non-state group, such as criminals or "hacktivists," that carries out operations helping a state while giving that state deniability.
10. **Norms of responsible state behaviour:** Voluntary rules agreed at the UN describing how states should act in cyberspace.
11. **Ransomware:** Malicious software that locks or steals data and demands payment to release it.
12. **Global Mechanism on ICT security:** The permanent UN body that replaced the temporary working groups on cyber security after 2025.

DISCUSSION QUESTIONS

1. Should a cyber operation that disables a system without physical damage, such as the Viasat or Kyivstar attacks, count as an "attack" under international humanitarian law?
2. Should civilian data, such as medical or banking records, receive the same protection as civilian buildings?
3. Is the rule of due diligence binding in cyberspace, or only a voluntary norm, and what reasonable steps should a state be expected to take?

4. How should international law hold a state responsible for proxy groups it encourages but does not formally control?
5. Does the world need a new binding treaty on state cyber operations, or should states focus on clarifying existing law through national positions?
6. When, if ever, can a cyber operation reach the level of an "armed attack" that allows self-defence under Article 51 of the UN Charter?
7. Should allied states be allowed to take collective countermeasures on behalf of a smaller state that was attacked?
8. How can the UN help developing countries write cyber laws and publish national positions so that they shape the rules rather than only follow them?