

HMDC Presents... LEGAL: Part 1 (The Topic)

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 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 "hacktivist" 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.