

HMDC Presents... LEGAL: Part 3 (International Efforts)

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 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?