

HMDC Presents... LEGAL: Review Quiz

HMDC Presents... Review Quiz: Legal Committee: Cyberwarfare Case Studies

We take this quiz after we finish reading the Legal Committee research report, not before. When we are done, we check our answers in the Answer Key at the end. For every question we missed, we go back to the part of the report named in the key and reread it until the reason makes sense.

PART 1, THE TOPIC

1. The Council on Foreign Relations Cyber Operations Tracker found that 34 countries are suspected of sponsoring cyber operations, and four of them account for 77 percent of suspected operations. What does this tell us?

- A. Cyber operations are rare events that happen only during wars.
- B. Cyber operations are a regular tool of state power, and a few states carry out most of them.
- C. Cyber operations are carried out mostly by criminal groups with no link to any state.
- D. Cyber operations stopped being a problem after 2019.

2. A Chinese state-sponsored group called Volt Typhoon hid inside communications, energy, transport and water networks, sometimes for years. Why did the agencies that studied it see this as more serious than ordinary spying?

- A. The group stole about \$1.5 billion in cryptocurrency.
- B. The group shut down the power grid in several countries at once.
- C. The agencies judged that the goal was to be ready to disrupt or destroy these systems in a future crisis or conflict.
- D. The group openly admitted that it was working for the Chinese government.

3. States disagree about what counts as an "attack" under the law of war. Which statement correctly describes the "expansive" group of states?

- A. It counts only operations that cause physical damage as attacks and usually does not protect data.
- B. It counts operations that cause a loss of functionality as attacks and protects essential civilian data.
- C. It says the law of war does not apply to cyber operations at all.
- D. It says only the Security Council can decide what counts as an attack.

4. Solution 1 asks states to publish "national positions" explaining how existing international law applies in cyberspace. What is one disadvantage of this solution?

- A. National positions require a long treaty negotiation before any state can publish one.
- B. Only 36 states have published positions, a small share of the 193 UN members.
- C. The ICRC has said that existing law offers no protection in cyberspace.
- D. National positions are binding and can be used to punish states that break them.

5. The African Union's Malabo Convention was adopted in 2014, entered into force only in 2023, and has been ratified by only 16 of 55 members. What lesson does this give a delegate who wants a new binding cyberwarfare treaty?

- A. Binding treaties always take effect within one year.
- B. Large states are always the first to ratify a new treaty.
- C. Signing a treaty is not the same as acting on it, and binding treaties can take close to a decade to take effect.
- D. Regional treaties never matter to the United Nations.

6. Solution 3 focuses on holding states and individuals accountable. Why does the use of "cyber proxies," such as criminal groups and hacktivists, make this harder?

- A. Proxies give a state deniability, and the legal bar for linking their conduct to a state is high.
- B. Proxies are always protected by the UN Convention against Cybercrime.
- C. Proxies only attack other proxies, so no state is ever harmed.
- D. International law forbids any state from sanctioning a proxy group.

PART 2, THE UNITED NATIONS

1. Resolution A/RES/53/70, adopted in 1998, holds a special place in the UN record on cyber security. What was it?

- A. The resolution that adopted the UN Convention against Cybercrime.
- B. The first UN action on information security, introduced by Russia and adopted without a vote.
- C. The resolution that created the permanent Global Mechanism on ICT security.
- D. The first resolution of the Sixth Committee on the law of war in cyberspace.

2. In 2018 the General Assembly created two kinds of groups on cyber security: a Group of Governmental Experts (A/RES/73/266) and an Open-ended Working Group (A/RES/73/27). What was the main difference between them?

- A. The expert group had 25 members, while the working group was open to all UN members.
- B. The expert group was open to all UN members, while the working group had only 5 members.
- C. The expert group studied cybercrime, while the working group studied sustainable development.
- D. The expert group was run by NATO, while the working group was run by the African Union.

3. Resolution A/RES/79/243 (December 24, 2024) adopted the UN Convention against Cybercrime. Why can it not simply be used to settle cyberwarfare disputes between states?

- A. It was rejected by every member of the General Assembly.
- B. It covers crime, not warfare between states.
- C. It applies only to countries in Europe.
- D. It was replaced by the Tallinn Manual in 2025.

4. Resolution A/RES/80/16 (December 1, 2025) endorsed the final report of the 2021-2025 Open-ended Working Group. What important change did it support?

- A. It ended all UN work on cyber security.
- B. It moved all cyber questions to the Security Council.
- C. It asked the Secretary-General to support the permanent Global Mechanism on ICT security starting in 2026.
- D. It made the 11 voluntary norms legally binding on every state.

5. Which UN body gives the Sixth Committee its most direct link to cyberwarfare, because it began studying "due diligence" in 2025?

- A. The International Law Commission.
- B. The Second Committee.
- C. The International Telecommunication Union.
- D. The Ad Hoc Committee on cybercrime.

PART 3, INTERNATIONAL EFFORTS

1. NATO adopted its first cyber defence policy after the 2007 attacks on Estonia. What did NATO agree in 2014?

- A. That cyber operations can never count as an armed attack.
- B. That a cyberattack could lead to invoking Article 5, its collective defence clause.
- C. That all members must sign the UN Convention against Cybercrime.
- D. That the Tallinn Manual is a binding treaty for all members.

2. The Council of Europe's Budapest Convention on Cybercrime has 83 parties, any state may join, and non-parties use it as a model law. What does this show?

- A. A regional treaty can become global over time.
- B. Regional treaties are always more popular than UN treaties.
- C. Only European states may take part in cybercrime treaties.
- D. The Budapest Convention covers attacks by states during war.

3. The International Counter Ransomware Initiative has 74 members and acted quickly against one specific harm. What is its main disadvantage, according to the report?

- A. It has no members from Asia.
- B. It is a binding treaty that most states refuse to sign.
- C. Only willing states join, so states accused of hosting ransomware groups are not part of it.
- D. It was shut down after its fifth summit in Singapore.

4. The Carnegie Endowment judged twenty years of UN cyber diplomacy. What gap did it point out in the 11 voluntary norms agreed in 2015?

- A. The norms were never agreed by any state.
- B. The norms are voluntary, carry no real accountability, and the ones that forbid certain actions are often ignored.
- C. The norms apply only to private companies, not to states.
- D. The norms were replaced by a binding treaty in 2021.

THINK LIKE A DELEGATE

These questions have no single correct answer. In a strong answer, we take a clear position, give a reason, and support it with at least one fact from the report.

1. We represent a small island developing state with limited technical capacity. What would we argue the committee should focus on, and why?

- 2. The Kyivstar attack disabled phone service for its 24 million customers, and after the Viasat attack, Viasat said tens of thousands of user terminals were damaged beyond repair. Should operations that shut down a service, or that damage equipment, count as an "attack" under international humanitarian law? Explain our reasoning.**
- 3. Should the world negotiate a new binding treaty on state cyber operations, or focus on clarifying existing law through national positions? Defend one choice.**

ANSWER KEY

PART 1, THE TOPIC

1. **B.** The report says cyber operations are a regular tool of state power and that a few states are responsible for most operations (Part 1, The Harms, Council on Foreign Relations Cyber Operations Tracker).
2. **C.** The agencies judged with high confidence that the goal was to be ready to disrupt or destroy these systems in a future crisis, not ordinary spying (Part 1, The Harms, CISA Joint Advisory AA24-038A).
3. **B.** The expansive group counts a loss of functionality as an attack and protects essential civilian data, while option A describes the restrictive group (Part 1, Solution 1, UNIDIR Publication, July 13, 2026).
4. **B.** The report notes that 36 states is a small share of the 193 UN members, so most states have not said what they believe the law requires (Part 1, Solution 1, Weighing this solution).
5. **C.** The Malabo record warns that signing is not the same as acting, and the report says binding treaties can take close to a decade to take effect (Part 1, Solution 2, Chatham House entries and Weighing this solution).
6. **A.** Proxies give Russia deniability, and the high legal bar for linking non-state conduct to a state means it often avoids responsibility (Part 1, Solution 3, Chatham House, March 25, 2026).

PART 2, THE UNITED NATIONS

1. **B.** The table lists A/RES/53/70 as the first UN action on information security, introduced by Russia and adopted without a vote (Part 2, Table of Resolutions).
2. **A.** The sixth Group of Governmental Experts had 25 members, while the first Open-ended Working Group was open to all UN members (Part 2, UNODA GGE Page and UNODA OEWG Page).
3. **B.** The report states that the convention covers crime, not warfare between states (Part 2, Table of Resolutions and UNODC Convention Page).
4. **C.** A/RES/80/16 asked the Secretary-General to support the Global Mechanism starting in 2026, giving cyber talks a permanent home instead of short-term groups (Part 2, Table of Resolutions and UN General Assembly Resolution A/RES/80/16).
5. **A.** The International Law Commission added "due diligence in international law" as a topic in 2025, and the Sixth Committee debates its reports every year (Part 2, introduction and UNIDIR Commentary, June 24, 2026).

PART 3, INTERNATIONAL EFFORTS

1. **B.** In 2014 NATO agreed that a cyberattack could lead to invoking Article 5, its collective defence clause (Part 3, NATO Cyber Defence Page).
2. **A.** The report says a regional treaty can become global over time, since any state may join and non-parties use it as a model (Part 3, Council of Europe Budapest Convention).
3. **C.** Only willing states join, so states accused of hosting ransomware groups are not part of the initiative (Part 3, Cyber Security Agency of Singapore).
4. **B.** The author says the norms are voluntary, carry no real accountability, and the ones that forbid certain actions are often ignored (Part 3, Carnegie Endowment for International Peace).

THINK LIKE A DELEGATE

1. **A strong answer includes:** a call for capacity building based on each country's own needs, as Micronesia argued at the Global Mechanism; the point that the UN must remain the main forum for inclusive dialogue; and support for help writing cyber laws and national positions. It may use the IMF finding that developing economies have the largest gaps in financial cyber rules (Part 2, Pacific Small Island States; Part 1, Solution 4; Part 1, The Harms, IMF Blog).
2. **A strong answer includes:** the split between the restrictive group (physical damage only) and the expansive group (loss of functionality counts); the scale of civilian harm in each case; and the ICRC view that core protections, such as the ban on targeting civilians, apply in cyberspace. It takes a side and explains how that choice would protect civilians or keep the rules realistic (Part 1, The Harms; Part 1, Solution 1).
3. **A strong answer includes:** for a treaty, the UN Convention against Cybercrime as proof that the UN can produce a binding cyber treaty, with 65 states signing on the first day; against a treaty, its slow ratification (only three states by July 2026) and the Malabo Convention's nine-year delay; and the Lieber Institute finding that states resist explaining how the law applies. A strong answer may propose the two-track approach the African Union used, a quick common position alongside a slower treaty (Part 1, Solutions 1 and 2; Part 2, Government of Canada).