

HMDC Presents... LEGAL: Quick Guide

LEGAL: QUICK GUIDE

Legal Committee (Sixth Committee): Cyberwarfare Case Studies

WHAT WE ARE DEBATING

Countries now use computers to attack other countries, which we call cyberwarfare. These attacks have hit power grids, hospitals, phone networks and water systems. We study real attacks and ask what the law says about them, and whether the world needs new and clearer rules.

WHAT OUR CHAIRS WILL FOCUS ON

1. **Real examples:** We study real cyberattacks between countries, which Harvard calls "an area of pressing potential threat."
2. **Size of the harm:** We judge how much each attack hurts people.
3. **Sets of rules:** We build sets of rules that make the harm smaller.
4. **Countries, not criminals:** We stay on attacks by countries, because the October session covered crime.

FIVE NUMBERS TO REMEMBER

1. **36:** Only 36 states have said in public how international law applies in cyberspace. (United Nations Institute for Disarmament Research, July 16, 2026)
2. **270,000:** Poland faced about 270,000 cyberattacks in 2025, about two and a half times as many as the year before. (Associated Press, March 24, 2026)
3. **19,000:** The WannaCry attack forced hospitals in England to cancel 19,000 or more medical appointments. (UK National Audit Office, October 27, 2017)
4. **\$2.5 billion:** The biggest cyber losses have grown more than four times since 2017, to \$2.5 billion. (International Monetary Fund, April 9, 2024)
5. **1,700:** In one Minnesota town, a water pump failed after an attack, and about 1,700 people were asked to save water. (NPR, August 12, 2026)

WHAT THE UN HAS ALREADY DONE

1. **A/RES/53/70 (1998):** This was the first UN action on information security, and Russia introduced it.
2. **A/RES/73/266 (2018):** This created a group of 25 experts, who agreed on a shared report in 2021.

3. **A/RES/79/243 (2024):** This adopted the first global cyber treaty, which covers crime and not war.
4. **A/RES/80/16 (2025):** This started the Global Mechanism, a lasting UN home for cyber talks from 2026.

THE MAIN SOLUTIONS

1. **Clarifying the laws we have:** Each country publishes how it believes today's laws apply in cyberspace.
 - Help: We build agreement step by step.
 - Harm: Only 36 of 193 countries have done this, so progress is slow.
2. **Writing a new treaty:** Countries sign a new set of rules that they must follow.
 - Help: Every country follows the same rules and can work together.
 - Harm: Treaties can take close to ten years to start.
3. **Holding attackers responsible:** Countries name the attacker and take hackers to court.
 - Help: Punishing attackers can stop others from trying.
 - Harm: Attackers often hide behind other groups, and they rebuild quickly.
4. **Helping every country defend itself:** Richer countries train poorer countries to protect their systems.
 - Help: Stronger defences lower the harm from every attack.
 - Harm: It is slow and depends on money given by other countries.

WHERE THE MAJOR BLOCS STAND

1. **United States:** The United States wants to punish attackers and says little about new international rules.
2. **China:** China says every country must follow the UN Charter and should control its own digital space.
3. **Russia:** Russia wants decisions made by all countries together and wants to talk about new agreements that countries must follow.
4. **European Union:** The EU says the 11 UN rules that countries choose to follow work together with laws they must follow, not in place of them.
5. **African Union:** All 55 African Union members agreed that breaking into another country's computer systems without permission is against the law.

KEY WORDS IN OUR TOPIC

1. **Attribution:** When we say attribution, we mean finding out which country carried out an attack.
2. **International humanitarian law:** When we say international humanitarian law, we mean the law of war, which protects ordinary people during war.
3. **Distinction:** When we say distinction, we mean that attacks may only aim at military targets, never at ordinary people.

4. **Proportionality:** When we say proportionality, we mean that harm to ordinary people must not be too large compared with what the army gains.
5. **Due diligence:** When we say due diligence, we mean that a country should not knowingly let its land be used to harm other countries.
6. **Sovereignty:** When we say sovereignty, we mean a country's power over its own land, including the computers inside it.
7. **Countermeasures:** When we say countermeasures, we mean actions that are normally not allowed, but are allowed to make a country stop breaking the law.
8. **Cyber proxy:** When we say cyber proxy, we mean a group, such as criminals, that attacks for a country so that the country can deny it.

QUESTIONS WE CAN ASK IN DEBATE

1. If an attack shuts down a phone network but breaks nothing, is it an "attack" under the law of war?
2. Should medical and bank records get the same protection as hospitals and banks themselves?
3. How does the delegate's plan hold a country responsible for hacker groups it helps?
4. Only three countries had fully approved the cybercrime treaty by July 2026, so why would a new cyberwarfare treaty move faster?

HMDC Forensics, Harvard MUN Online, December 2026