

HMDC Presents... LEGAL: Sample Draft Resolution

HMDC Presents... Sample Draft Resolution: Legal Committee: Cyberwarfare Case Studies

THIS IS A MODEL TO LEARN FROM, NOT TO COPY. A resolution is written by the whole bloc during committee, not at home. We study this sample at home to learn the shape of a resolution and the kind of ideas that belong in it. Then we write every clause live, in our own words, with our bloc.

HOW A RESOLUTION IS BUILT

A resolution has two kinds of clauses. **Preambulatory clauses** come first: they explain why the committee is acting by recalling past resolutions, treaties and facts. Each one begins with an *italic* opening word or phrase, such as *Recalling* or *Deeply concerned*, and ends with a comma.

Operative clauses come second: they say what the committee will actually do. Each one is numbered, begins with a **bold** (or underlined) verb, such as **Encourages** or **Requests**, and ends with a semicolon, except the final clause, which ends with a period. The Legal Committee is part of the General Assembly, so it recommends and requests rather than commands. Its strongest tools are clear legal wording and requests to UN bodies such as the International Law Commission.

THE SAMPLE DRAFT RESOLUTION

Committee: Legal Committee (Sixth Committee of the General Assembly) **Topic:** Cyberwarfare Case Studies **Sponsors:** The Republic of Mauritius, the Federated States of Micronesia, the Commonwealth of Australia **Signatories:** [signatories]

The Sixth Committee,

Recalling General Assembly resolution 73/266 (2018) on advancing responsible State behaviour in cyberspace, and the consensus report of the sixth Group of Governmental Experts (A/76/135) together with its compendium of national views on international law (A/76/136),

Reaffirming that all States have agreed that existing international law applies to State conduct in cyberspace, and that the 2025 final report of the Open-ended Working Group (A/80/257) recorded agreement on sovereignty, non-intervention, the prohibition of the use of force and the peaceful settlement of disputes,

Welcoming resolution 80/16 (2025), which endorsed that report and asked the Secretary-General to support the Global Mechanism on ICT security and responsible State behaviour from 2026,

Noting with interest that in 2025 the International Law Commission added "due diligence in international law" to its work, and that its Special Rapporteur's first report of April 2026 discussed possible application to cyberspace,

Recognizing the Common African Position adopted in January 2024 by all 55 members of the African Union, and the 36 States and two regional organizations that have published national positions on international law in cyberspace,

Recalling also the United Nations Convention against Cybercrime, adopted by resolution 79/243 on December 24, 2024, which shows that Member States can agree binding rules for cyberspace,

Deeply concerned that cyber operations have cut phone service for 24 million customers in Ukraine, disrupted at least 81 hospital trusts in England, and struck a heat and power plant in Poland that serves nearly 500,000 customers in winter,

1. **Encourages** all Member States that have not yet done so to publish a national position on how international law applies to their conduct in cyberspace;
 2. **Requests** the United Nations Institute for Disarmament Research, working with regional organizations such as the African Union and the Association of Southeast Asian Nations, to offer legal training and practice exercises to any State that asks for help preparing its national position, following the principle that support should be requested by the country and fit its needs;
 3. **Recommends** that the Global Mechanism on ICT security test how existing international law applies to concrete cyber incident scenarios, beginning with:
 - a. Whether an operation that causes a loss of functionality, without physical damage, counts as an "attack" under international humanitarian law;
 - b. Whether essential civilian data, such as medical and banking records, is a civilian object that must not be targeted;
 - c. When hidden access to another State's water, energy or communications systems in peacetime breaks the rules of sovereignty and non-intervention;
 4. **Affirms** that international humanitarian law, including the rules of distinction and proportionality and the duty to protect medical services, applies to cyber operations during armed conflict, and that this affirmation in no way makes any armed conflict legitimate;
 5. **Calls upon** Member States to take reasonable steps so that their territory is not knowingly used for cyber operations that harm other States, noting that this duty does not require the monitoring of all activity;
 6. **Invites** the International Law Commission to give special attention to cyberspace in its continuing study of due diligence and to share its findings with the Sixth Committee;
 7. **Urges** Member States to update their national laws so that war crimes, crimes against humanity, genocide and aggression committed fully or partly through cyber means can be investigated and prosecuted, and notes the December 3, 2025 Policy on Cyber-Enabled Crimes of the Office of the Prosecutor of the International Criminal Court;
 8. **Encourages** States and donors to support legal and technical capacity building through existing networks, such as the Global Forum on Cyber Expertise, giving priority to developing States and small island developing States with limited technical capacity;
 9. **Decides** to continue its consideration of the application of international law to State conduct in cyberspace at a future session.
-

HOW WE MERGE AND AMEND IN COMMITTEE

1. **Merging with a treaty bloc:** Russia wants the Global Mechanism to discuss "the possibility of developing legally binding agreements" (UN Office for Disarmament Affairs, October 27, 2025). So a treaty bloc may write a paper that does not match this sample. We can offer to merge by adding a clause that asks the Global Mechanism to study a binding treaty later. We keep our clauses on national positions and on testing the law against real incidents. Both papers then become one resolution with more votes.
2. **Choosing words that can pass:** The 2025 working group warned against using the law of war in a way that could make conflict seem legitimate (Lieber Institute for Law and Warfare, January 9, 2026). We learn from this: clause 4 above affirms that the law of war applies and then adds that this does not make any conflict legitimate, which helps cautious delegations vote yes.
3. **Amending through the right steps:** An amendment is a change to a clause after the paper is written. Each committee has its own rules for amendments, so we listen to the dais when it explains them. If the dais has not explained them, we raise a point of parliamentary inquiry before we write an amendment.

HMDC Forensics, Harvard MUN Online, December 2026

HMDC Forensics, Harvard MUN Online, December 2026