

## HMDC Presents... LEGAL: Video 2 Transcripts

These are the words spoken in the two Video 2 films for LEGAL (The United Nations and International Efforts). We read along while we watch, pause at each time mark, and circle any word we do not know so we can look it up together.

### VIDEO 2 (EXPLAINER)

---

**[0:00]** Welcome, delegates. I am so thrilled to guide you through this explainer on cyber warfare case studies today. We are focusing on the record of the United Nations. We will also look at the work of other international actors. Our goal is to prepare you for the legal committee. We want you to understand exactly where the law stands today. The information ahead will help you debate clearly. It will also help you write strong working papers. OK, let's dive into this. Here is our agenda for today. First, we have the UN cyber record. Second, treaties and legal links. Third, consensus versus deep divisions. Fourth, roles of international actors. Fifth, remaining gaps in cyberspace. And sixth, a closing committee challenge. This structure is definitely going to help you organize your notes efficiently.

**[0:46]** So let's start with section one, the UN cyber record. The UN actually has a really long record of addressing information security. According to the UN Office for Disarmament Affairs, last accessed October 2026, the very first action took place in 1998. This was done through resolution A slash RES slash 53 slash 70. This same UN Office for Disarmament Affairs source notes that since 2004, the UN has used six groups of governmental experts. It also confirms that four of these groups produced consensus reports. Over time, the UN moved from small expert groups to talks open to all member states. According to UNIDIR, April 8, 2026, the sixth expert group was created by resolution A slash RES slash 73 slash 266. This same UNIDIR report states this group had 25 members and produced report A slash 76 slash 135. Furthermore, this 2026 UNIDIR source explains the first open-ended working group was created by resolution A slash RES slash 73 slash 27. It notes this group adopted its final report on March 12, 2021. Finally, this UNIDIR text details the second working group. It was created by resolution A slash RES slash 75 slash 240. The text states this second group met in 11 sessions, where more than 130 delegations actually spoke.

**[2:08]** All of this temporary work led to a brand new structure. The UN created a permanent forum. This is called the Global Mechanism on ICT Security. According to UNIDIR July 21, 2026, this mechanism was meeting in mid-2026. This permanent body represents a major step forward for international cooperation. Moving right along to Section 2, treaties and legal links. According to UNODC last accessed October 2026, the General Assembly adopted the Convention Against Cybercrime on December 24, 2024. This treaty needs 40 parties to enter into force. It is important to note that this treaty covers crime rather than warfare between states. However, states hold very different opinions on this new text. According to UN press release GA slash 12671, divided views emerged during the convention's adoption.

**[2:59]** Russia's delegate stated that negotiations were tense. This delegate also requested additional protocols. In contrast, Vietnam's delegate praised the treaty. They called it the first international legal instrument governing cyberspace. This brings us directly to the work of the Sixth Committee. Your committee often debates the principle of due diligence. Due diligence is the principle that a state should not knowingly allow its territory to be used to harm other states. According to UNIDIR June 24, 2026, the International Law Commission began studying this topic in 2025. This UNIDIR report discusses its application to cyberspace. You can definitely use this legal connection to build stronger arguments in your working papers. Next up is Section 3, consensus versus deep divisions. Now, what's really interesting about this slide is how we can analyze these viewpoints. We can easily contrast the desirable outcomes with the undesirable realities here.

**[3:54]** According to UNIDIR September 18, 2026, it is highly desirable that states agree that international law applies. It is also desirable that rival powers can reach consensus on principles. However, the current divisions are undesirable. Having no shared meaning of an attack is completely undesirable. A split over voluntary norms versus binding law is also undesirable. These disagreements cause harm by leaving civilians unprotected. Let's look at Section 4, roles of international actors. Many different actors provide help in cyberspace to fill these legal gaps. For example, NATO treats serious cyber operations as collective defense. Meanwhile, the European Union helps by publicly naming the responsible state. In the legal realm, the Council of Europe spreads binding law through its Budapest Convention. Similarly, the African Union shapes regional law with its own cyber treaty. Finally, the Tallinn Manual adds value by explaining international law in great detail. Beyond organizations, specific initiatives also help build security. The Paris Call brings companies into voluntary declarations. Taking a different approach, the Pall Mall process aims to limit commercial hacking tools. Around the world, the Global Forum on Cyber Expertise coordinates capacity building. The Oxford process contributes by drafting legal statements on specific harms. Lastly, the non-state group Protect.NGO helps by defending victims directly.

**[5:19]** This brings us to Section 5, remaining gaps in cyberspace. Critical gaps remain open today, which your committee simply must address. First, voluntary codes create no binding duties. Second, international law does not clearly ban spying. The Salt Typhoon breaches are a clear example of this spying. Third, proxy groups often escape responsibility. This makes it very difficult to hold states accountable. The financial harm from these gaps is massive. According to CSIS Significant Cyber Incidents, last accessed October 2026, North Korean hackers stole \$1.5 billion from Bybit. This same CSIS source notes this massive theft occurred in February 2025. This event clearly demonstrates the danger of sanctions-busting theft.

**[6:05]** And finally, Section 6, a closing committee challenge. I want to leave you with a direct question to think about. Where can a new resolution from the legal committee add real value? You must decide if you want to clarify existing law or demand new binding treaties. You must decide how to address due diligence and capacity building. Review this information, debate these points, and draft your working papers with absolute confidence. Thank you for joining me on this explainer, and I wish you all incredible success in committee.

## VIDEO 2 (CINEMATIC)

---

**[0:00]** For nearly 30 years, the United Nations has tried to govern cyberspace. Yet today, state-sponsored hackers routinely target power grids and hospitals, operating in a digital domain that remains a largely untamed legal frontier. The diplomatic paper trail actually starts back in 1998, when the very first UN resolution addressing information security was introduced. To tackle this new threat, the UN relied on a small-room strategy. They assigned the problem to a group of governmental experts, a highly curated committee restricted to exactly 25 member states. This approach yielded a genuine diplomatic breakthrough. Rival powers, specifically China, Russia, and the United States, sat at the same table and managed to agree on a series of foundational reports.

**[0:48]** The most crucial principle they locked down was simple but vital. Existing international law, including the UN Charter, applies directly to state behavior in cyberspace. That early era proved international consensus was entirely possible, provided you restricted the conversation to a tiny fraction of global powers and focused on broad, overarching principles, rather than specific enforceable rules. Eventually, the process had to modernize. The UN transitioned away from those 25 isolated experts and created the open-ended working group, opening the microphones to more than 130 global delegations. The physical and institutional scale of this inclusion positioned the UN General Assembly as the undisputed center of global cyber lawmaking.

**[1:35]** The peak achievement of this massive, multi-year diplomatic engine arrived in late 2024, when the General Assembly successfully negotiated and adopted the first ever UN cyber treaty, specifically targeting cybercrime. The UN successfully built the machinery to include the entire world in the conversation. However, maintaining consensus across that many nations has masked a critical failure in defining the underlying law of war. The core crisis paralyzing the legal committee today is definitional. After more than a decade of active talks, the world's nations still cannot agree on what exactly constitutes a cyber attack. The UN is split between two legal interpretations. A restrictive group of states argues that an operation is only an attack if it causes actual physical damage.

**[2:24]** An expansive group argues that causing a loss of digital functionality should also trigger the laws of armed conflict. By relying solely on the restrictive definition, essential civilian data, like banking records and medical databases, is left entirely unprotected because deleting data doesn't physically destroy the hard drives. This gap has immediate consequences. In December 2023, a cyber operation hit Kyivstar, Ukraine's largest mobile provider, cutting phone and emergency services for 24 million civilians. Legally, the operation sits in a gray area because it didn't blow up the cell towers. Without a universally accepted definition of an attack, the central UN framework remains structurally paralyzed when it comes to governing the reality of modern state-sponsored digital warfare.

**[3:14]** Nature abhors a vacuum. Because the UN cannot define the terms of digital war, the periphery is now writing its own rules. The NATO Military Alliance established its own aggressive legal threshold, declaring that cumulative cyber activities could trigger Article 5 collective defense. In the global south, the African Union is actively shaping its cyber sovereignty, adopting regional agreements, and issuing common African positions on international law. Private companies are also stepping into the governance void. Initiatives like the Paris Call gather tech firms and willing governments into voluntary agreements designed to regulate commercial hacking tools and private cyber mercenaries. These regional and corporate efforts provide immediate stopgaps for a vulnerable internet.

**[4:01]** But a fractured, non-binding patchwork is no substitute for universal international law. The beneficiaries of this fragmented legal landscape are rogue state-sponsored hackers and proxy groups. They actively exploit these jurisdictional gray areas to operate with near impunity. The economic toll is staggering. Hackers breached an exchange and extracted roughly \$1.5 billion, funneling vast wealth past international sanctions. Cyber risk rises in direct tandem with geopolitical tension. When these legally undefined digital operations go unchecked, they threaten to escalate into conventional global conflicts. This leaves the delegates of the UN's 6th Committee with an urgent burden.

**[4:47]** They must either definitively clarify how existing laws apply to the digital domain, or negotiate a bold new treaty to repair the center, before the periphery spirals entirely out of control.