

HMDC Presents... LEGAL: Video 1 Transcripts

These are the words spoken in the two Video 1 films for LEGAL (The Topic). 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 1 (EXPLAINER)

[0:00] Welcome delegates to this explainer. Cyber warfare is absolutely reshaping our world. Today, we are going to break down this complex topic. We will stick to one clear idea per sentence. This steady pace is going to help you prepare for Harvard MUN Online. That conference takes place on December 5th and 6th, 2026. Let's get started. Here is our agenda for today. It acts as our roadmap. We will cover the legal committee's central question, the scale of cyber harms, two crucial legal definitions, four major potential solutions, lesser solutions and emerging threats, and finally, the closing delegate challenge. Section 1 covers the legal committee's central question. So what is this committee?

[0:45] Well, the legal committee is the sixth committee of the General Assembly. It holds a very important role. It serves as the primary United Nations forum for international legal questions. Literally, this is where global rules are debated. This committee faces a vital central question. Does existing international law already cover state cyber operations? Now, existing law includes the UN Charter. It also includes state responsibility and international humanitarian law. However, some delegates claim relying on these old laws is incorrect. They argue that cyber operations are entirely new. Therefore, they believe the world needs new rules to prevent harm. Moving right along to section two, the scale of cyber harms. State cyber operations are incredibly common today.

[1:31] In fact, 34 countries are suspected of sponsoring these operations. We know this from the Council on Foreign Relations last accessed October, 2026. Interestingly, a tiny fraction of states cause most of the damage. Just four states are responsible for 77% of these operations. This fact is also according to the Council on Foreign Relations last accessed October, 2026. Let us examine these specific harms chronologically. The damage can be truly devastating. For example, the WannaCry attack affected 81 hospital trusts. It even canceled 19,000 appointments. This specific data comes from the UK National Audit Office published on October 27th, 2017. The financial cost is also massive. The NotPetya attack caused nearly \$1 billion in losses across just three victims.

[2:16] The US Department of Justice reported this on October 19th, 2020. Infrastructure is highly vulnerable too. The Viasat attack damaged tens of thousands of satellite terminals. This is according to gov.uk on May 10th, 2022. Entire nations can actually be paralyzed. Massive attacks recently hit Costa Rica and Albania. This is according to CSIS last accessed October, 2026. In another shocking case, the Kyivstar attack cut service for 24 million customers. That is also noted by the same CSIS publication last accessed October, 2026. Finally, threats can remain completely hidden. A group called Volt Typhoon hid quietly inside infrastructure systems. CSIS warned of this on February 7th, 2024 [Our report says: CISA, the U.S. Cybersecurity and Infrastructure Security Agency]. The Viasat attack highlights two vital legal terms for us.

[3:03] The first term is distinction. Distinction means separating military targets from civilian targets. The second term is proportionality. Proportionality means harm to civilians must not be excessive compared to the military advantage gained. So when cyber attacks spill over and damage civilian terminals, these two principles are seriously tested. We also absolutely must understand sovereignty. Sovereignty is a state's absolute authority over its own territory and systems. Recall the Volt Typhoon case we just mentioned. That group hid inside foreign systems to prepare for future attacks. Again, we learned this from CSIS on February 7th, 2024 [Our report says: CISA]. Invading a network like this definitely challenges a state's sovereignty, even during peacetime. That brings us to section three, two crucial legal definitions.

[3:49] Delegates face deep divisions over two specific definitions. First, states divide over what actually counts as an attack. A restrictive group of states requires actual physical damage. On the other hand, an expansive group argues that a mere loss of functionality counts as an attack. Second, states divide over whether essential civilian data receives legal protection. Both of these deep divisions are outlined by UNIDIR, published July 13th, 2026. Let's jump into section four, four major potential solutions. There are four major solutions currently on the table. The first solution is clarifying existing law. This is desirable because 36 states have already published national positions. However, it is undesirable because it excludes most of the 193 UN members.

[4:35] We know these specific numbers from UNIDIR, published July 16th, 2026. The second solution is a new binding treaty. This is desirable for creating shared legal channels, but it is undesirable because treaties are notoriously slow to ratify. The third solution is accountability. Charging individual hackers is highly desirable. Yet it is undesirable because collecting solid digital evidence is very hard. The fourth solution is capacity building. Helping weaker states defend themselves is a desirable goal. The undesirable reality is that this depends heavily on voluntary donor funding. To pursue accountability, we must understand three major bottlenecks. First is attribution. Attribution simply means naming the responsible state. Second is countermeasures.

[5:20] Countermeasures are lawful responses to violations, designed to make the violations stop. Finally, we must define cyber proxy. A cyber proxy is a deniable non-state actor. States often use these proxies to avoid direct attribution. Section five covers lesser solutions and emerging threats. Delegates must also look to the future. One lesser solution involves regulating the commercial hacking tool market. Chatham House proposed eight principles for this regulation. They published this on October 18th, 2024. Another massive challenge is preparing for AI-assisted attacks. Advanced AI models will make cyber threats much faster and stronger. Chatham House warned about this specific threat on June 3rd, 2026. Finally, section six is the closing delegate challenge.

[6:08] You have reviewed the devastating scale of these harms. You have seen the proposed solutions. You now know the crucial legal terms. The choice is completely in your hands. So which solution will your country support and why? I hope this explainer helps you succeed in committee. Good luck, delegates.

VIDEO 1 (CINEMATIC)

[0:00] A string of code typed on one continent can jump a border in milliseconds and black out a power grid on another. When a state launches an attack with malware instead of missiles, the United Nations' Sixth Committee faces a blank spot in international law. Data from the Council on Foreign Relations tracks 34 countries suspected of sponsoring these operations. Just four of them—China, Russia, Iran, and North Korea—account for 77% of the activity. These operations are a regular, dominant tool of state power, operating entirely within a massive legal gray area. In December 2023, Russian hackers decimated the network of Kyivstar, Ukraine's largest mobile provider. 24 million civilians suddenly lost access to phone service, family check-ins, and emergency dispatch during an active, kinetic war.

[0:52] International humanitarian law relies on a principle called distinction—the strict legal requirement to separate legitimate military targets from civilian objects. But code rarely respects boundaries. An hour before the invasion of Ukraine, a targeted strike on the Viasat satellite network spilled across borders. It knocked out thousands of user terminals and disabled wind farms deep in Central Europe. The human cost extends to medicine. This website notice from an English hospital trust is a direct result of the 2017 WannaCry ransomware attack. The malware crippled 81 hospital trusts and forced the cancellation of at least 19,000 medical appointments. That same year, a single destructive malware variant, known as NotPetya, caused nearly \$1 billion in economic damages to just three of its corporate victims.

[1:40] These weapons do not differentiate between soldiers and civilians. And their reach is borderless. They directly violate the protective spirit of the laws of war. A state-sponsored group known as Volt Typhoon infiltrated the communications, transport, and water networks of foreign nations and hid there for years. The goal is pre-positioning, lying in wait to sabotage critical systems during a future crisis. This raises a difficult question about sovereignty. If a foreign state embeds dormant code inside your civilian water supply during peacetime, is that an act of espionage? Or is it an attack? In 2022, hackers crippled Costa Rica's Ministry of Finance, shutting down tax collection and exports. Years later [Our report says: July and September 2022, the same year], Iranian actors destroyed Albanian government data and disabled their entire border tracking system.

[2:30] States now possess the capability to paralyze a nation's government infrastructure without firing a single physical bullet. Despite the billions in damage and the disruption to millions of lives, international law remains trapped by a crisis of definition. Under the law of war, member states are strictly divided over what constitutes an attack. A restrictive group argues that an operation must cause literal physical damage to count. An expansive group argues that causing a massive loss of system functionality should also qualify. If an attack is only recognized by broken concrete and fire, then a piece of code that silently wipes a country's banking servers and civilian medical records is technically not an act of warfare, leaving that data completely legally unprotected.

[3:15] The United Nations has spent decades trying to resolve this. They have convened small groups of governmental experts and launched massive open-ended working groups open to all 193 members. Yet the speed of technological escalation drastically outpaces diplomatic consensus, leaving the world's most critical infrastructure legally defenseless. Delegates in the 6th Committee have four main paths to pursue. The first is to clarify existing law by pushing states to publish formal national positions on exactly how the UN Charter applies in cyberspace. This relies entirely on voluntary participation. Currently, only 36 states have published these positions, leaving the vast majority of the UN silent. The second path is to develop voluntary norms, which are non-binding rules of the road that shape how states behave.

[4:04] A third option involves focusing on practical capacity building, especially for developing nations. Finally, the Committee can choose to pursue an entirely new treaty specifically for cyberspace. The second path is to negotiate new binding treaties. The UN proved rapid drafting is possible when it finalized the Convention Against Cybercrime in roughly four years. Writing a treaty is fast. Ratifying it is not. The African Union adopted the Malabo Convention on Cybersecurity in 2014, but it took nine years just to enter into force. A third route enforces accountability through targeted criminal charges and financial sanctions. This directly penalizes the proxy hacking groups that give aggressive states plausible deniability.

[4:50] The final option bypasses the legal stalemates entirely to focus on physical defense. Using tools like the ITU Global Cybersecurity Index, this path directs resources and capacity building to help developing nations fortify their own networks. The Committee faces a difficult choice. Patch up a fragmented set of existing laws, or attempt to forge an entirely new global consensus from scratch. Global cyber risk rises in direct correlation with geopolitical tension. As a delegate in the sixth committee, you must decide which legal mechanism your country will prioritize to secure the digital domain. Failing to define the rules of cyber conflict today ensures that civilians will bear the brunt of the next undeclared war tomorrow.