# Background Guide

## LEGAL

Duke

# Letter from the Chair

Dear Delegates,

Welcome to the Sixth Committee (Legal) at DUMUNC! We're thrilled to guide you through debates on two of the most complex legal questions of our time.

International law is often called a "living system" because it evolves as the world changes. Our topics represent exactly the kind of evolution the law must undergo. When the Geneva Conventions were written, no one imagined armies of hackers attacking hospitals from thousands of miles away. When the International Criminal Court was established, its framers focused on state armies and rebel groups, not the loose networks of violent extremists we see today.

The Sixth Committee is where international law gets made. The treaties and conventions that govern how nations and individuals behave often start as draft articles debated in this room. Your work here isn't academic; it shapes the rules that determine responsibility when a state's hackers paralyze another country's power grid, or when a terrorist organization commits atrocities.

Come ready to wrestle with hard questions. International law rarely offers easy answers.

Best regards,

Committee Leadership

LEGAL (Sixth Committee)

# History of the Committee

The Sixth Committee (commonly called the Legal Committee) is one of six main committees of the United Nations General Assembly. It serves as the UN's primary forum for international law, handling everything from treaty interpretation to the development of entirely new legal frameworks. All 193 UN member states participate, giving every nation a voice in shaping the rules that govern international conduct.[1]

The committee's mandate comes directly from the UN Charter. Article 13 charges the General Assembly with "encouraging the progressive development of international law and its codification." The Sixth Committee fulfills this mandate by reviewing the work of the International Law Commission (ILC), a body of legal experts that drafts new treaties and clarifies existing law. Many foundational treaties (from diplomatic immunity to the law of the sea) began as ILC draft articles debated in the Sixth Committee.[2]

The committee meets annually alongside the General Assembly session, with "International Law Week" in late October being the highlight. During this week, the world's top legal advisers gather to debate the ILC's annual report. The committee also addresses specific legal issues as they arise, from terrorism to cybercrime to the scope of state immunity. Its resolutions shape how international law evolves in response to new challenges.[3]

# Topic A: Defining State Responsibility for State-Sponsored Cyber Warfare

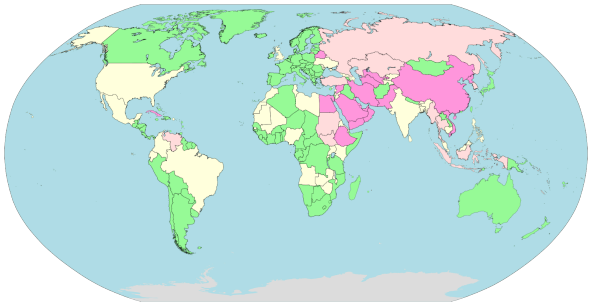
## Statement of the Problem

When does a cyberattack become an act of war? Who's responsible when hackers working for a government disable hospitals, shut down power grids, or interfere with elections? These questions sit at the intersection of technology and international law, and right now, the answers are disturbingly unclear.

Cyberattacks on critical infrastructure have become routine. In 2024, Ukraine's government recorded 4,315 cyber incidents (a 70% increase from the previous year) targeting government systems, energy infrastructure, and telecommunications. Russian state-sponsored hackers attacked heating systems in Lviv during sub-zero temperatures, leaving residents without heat. Similar attacks have targeted hospitals, water treatment plants, and financial systems across multiple countries.[4]

The problem isn't just Russia. States around the world use cyber operations as instruments of foreign policy. China-linked groups have targeted Tibetan activists and Western government agencies. North Korean hackers have stolen billions in cryptocurrency. Iran has attacked banks and infrastructure in the Gulf states. These operations exist in a legal gray zone: clearly hostile, but difficult to categorize under traditional frameworks designed for conventional warfare.[5]

International law struggles with cyberattacks for several reasons. First, attribution is hard. Unlike a missile, which leaves physical evidence of its origin, cyberattacks can be routed through servers in multiple countries, making it difficult to prove who's responsible. States typically deny involvement, blaming "patriotic hackers" or criminal groups. Second, the rules are unclear. The UN Charter prohibits the "use of force" against other states, but does a cyberattack that causes no physical damage count as "force"? What about one that causes deaths by disabling hospital systems? Third, enforcement is nearly impossible. Even when attribution is clear, there's no international court with jurisdiction over state cyber operations.[6]



The result is what some scholars call "cyber anarchy," a domain where states can attack each other with relative impunity, constrained only by the fear of retaliation. The question for delegates: how can international law bring order to cyberspace?

## History of the Problem

The internet wasn't built with security in mind. Developed by academics and researchers in the 1960s and 70s, it was designed for open information sharing, not for protecting critical infrastructure from hostile states. As governments and essential services moved online, they inherited this fundamental vulnerability.

The first major state-sponsored cyberattack to shape international law discussions was the 2007 assault on Estonia. Following a political dispute with Russia over a Soviet-era war memorial, Estonian government websites, banks, and media outlets were overwhelmed by coordinated denial-of-service attacks. The

country, one of the world's most digitized, was partially paralyzed for weeks. Russia denied involvement, and attribution proved difficult. The attacks weren't destructive in the traditional sense, but they demonstrated how cyber operations could cripple a modern state.[7]

This event prompted serious thinking about how international law applies to cyberspace. NATO's Cooperative Cyber Defence Centre of Excellence in Tallinn commissioned a group of legal experts to study the question. The result was the Tallinn Manual (2013), an academic analysis of how existing international law applies to cyber warfare. The manual's 95 rules addressed questions from sovereignty to armed conflict. While non-binding, it became the most influential reference on cyber law.[8]

The Tallinn Manual 2.0 (2017) expanded the analysis to peacetime cyber operations: espionage, data theft, and attacks below the threshold of armed conflict. It established 154 rules covering sovereignty, state responsibility, human rights, and jurisdiction. A third edition is currently in development.[9]

Meanwhile, cyber operations became increasingly sophisticated and destructive. The 2010 Stuxnet worm (developed by the U.S. and Israel) physically destroyed Iranian nuclear centrifuges, demonstrating that code could cause real-world damage. Russia's 2015 and 2016 attacks on Ukraine's power grid left hundreds of thousands without electricity. The 2017 NotPetya malware, aimed at Ukraine, spread globally and caused over $10 billion in damage to shipping companies, pharmaceutical manufacturers, and other businesses.[10]

The UN has addressed cyber issues through multiple forums. The Group of Governmental Experts (GGE) on information security issued reports in 2013, 2015,

and 2021 affirming that international law applies to cyberspace. The Open-Ended Working Group (OEWG) has brought more states into the discussion. In 2024, the UN adopted its first Cybercrime Convention, though it focuses on criminal activity rather than state-sponsored operations.[11]

Despite this progress, fundamental questions remain unresolved. When does a cyberattack constitute an "armed attack" justifying self-defense? What standard of evidence is required to attribute an attack to a state? What remedies exist for states that are victims of cyber operations? The law remains far behind the technology.

## Past Actions

The Tallinn Manuals: While not official UN documents, these academic analyses have become the most cited authority on cyber law. The manuals apply existing international law principles (sovereignty, non-intervention, use of force) to cyber operations. States increasingly reference them when articulating their own legal positions.[12]

UN Group of Governmental Experts (GGE): Since 2004, successive GGE reports have built consensus that international law applies to cyberspace. The 2015 report established eleven voluntary norms for responsible state behavior, including that states shouldn't attack critical infrastructure or harm computer emergency response teams. However, the GGE operates by consensus and has struggled to address difficult questions about how law applies in practice.[13]

UN Open-Ended Working Group (OEWG): Created in 2018 to complement the GGE with more inclusive participation, the OEWG has brought developing countries into

cyber diplomacy. Its mandate extends through 2025, with discussions on establishing a permanent UN mechanism for cyber issues. The 2024 session addressed emerging threats from AI-enhanced cyberattacks.[14]

Regional Initiatives: The European Union adopted a declaration on international law in cyberspace in November 2024, the first time the EU collectively articulated how it interprets cyber law. The African Union adopted its Common African Position in January 2024. These regional positions help build the state practice that shapes customary international law.[15]

Articles on State Responsibility: The International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts (2001) provide the framework for attributing conduct to states. Under these articles, a state is responsible for cyber operations conducted by its organs or by actors operating under its "direction or control." The challenge is applying this framework to the murky world of state-sponsored hacking groups.[16]

## Possible Solutions

An International Attribution Body: The biggest barrier to accountability is proving who's behind an attack. An independent body (like the IAEA for nuclear issues or OPCW for chemical weapons) could investigate major cyber incidents and issue findings. States might still dispute the conclusions, but a credible third party would make denial harder and strengthen the basis for response.

Defining "Cyber Armed Attack": The UN Charter allows self-defense against "armed attacks," but that term was written for missiles and troops. A General Assembly resolution or ILC study could clarify when cyber operations cross this line, perhaps when they cause physical destruction, significant casualties, or sustained damage to critical infrastructure. Clear rules would reduce dangerous ambiguity.

Incident Response Protocols: States could commit to notifying each other of major cyber incidents and cooperating in investigations. This won't prevent attacks, but it would create norms for de-escalation. When a state refuses to cooperate or investigate attacks originating from its territory, its bad faith would be visible.

# Topic B: Establishing Individual Criminal Liability for War Crimes Committed by Non-State Actors

## Statement of the Problem

International humanitarian law was written for wars between armies. It assumes organized forces with clear command structures, wearing uniforms, following orders. But many of today's most brutal conflicts involve groups that don't fit this model: terrorist organizations, militias, warlords, and armed gangs that commit atrocities without regard for legal niceties.

The scale of violence by non-state actors is enormous. The Sahel region has become a battleground between governments and terrorist groups like Islamic State affiliates and al-Qaeda's JNIM. In 2024, these groups were responsible for over half of all terrorism-related deaths worldwide. In Syria, multiple non-state armed groups have committed documented war crimes over more than a decade of conflict. In the Democratic Republic of Congo, dozens of armed groups operate with varying degrees of organization and brutality.[17]

International criminal law has made progress in holding individuals accountable. The International Criminal Court has issued warrants for leaders of armed groups, including Hamas military commanders and Taliban leaders. In 2024, the ICC convicted Al Hassan Ag Abdoul Aziz for war crimes and crimes against humanity committed in Mali while he was part of the armed groups Ansar Dine and Al-Qaeda in the Islamic Maghreb.[18]

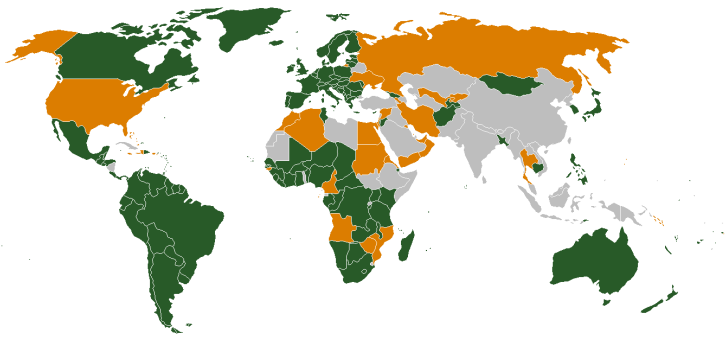
But significant gaps remain. The ICC can only exercise jurisdiction when the state where crimes occurred is a party to the Rome Statute or when the Security Council refers a situation, and Security Council referrals are often blocked by vetoes. The court lacks its own enforcement mechanism; it depends entirely on states to arrest suspects. Many armed group leaders operate in regions where no state has the capacity or will to arrest them.[19]

There's also a conceptual problem. Traditional war crimes law distinguishes between international armed conflicts (between states) and non-international armed conflicts (within states). Different rules apply to each. Many non-state actor conflicts don't fit neatly into either category: groups operate across borders, lack territorial control, or have ambiguous relationships with states. The law struggles to keep up with the reality of modern armed conflict.[20]

The question for delegates: how can international criminal law more effectively hold non-state actors accountable for war crimes and crimes against humanity?

## History of the Problem

The idea that individuals (not just states) can be held criminally responsible for violations of international law is relatively new. For most of history, international law governed relations between sovereigns. Individuals were subject only to their own national laws.



The Nuremberg and Tokyo tribunals after World War II changed this. For the first time, individuals were tried for "crimes against peace," war crimes, and "crimes against humanity" under international law. The Nuremberg judgment established that "crimes against international law are committed by men, not by abstract entities, and only by punishing individuals who commit such crimes can the provisions of international law be enforced."[21]

The Geneva Conventions of 1949 codified the laws of war, including protections for civilians and prisoners. Crucially, Common Article 3 extended basic protections to non-international armed conflicts, including civil wars and insurgencies. This meant that non-state armed groups were bound by at least minimum humanitarian standards. Additional Protocol II (1977) elaborated these rules for conflicts between governments and organized armed groups.[22]

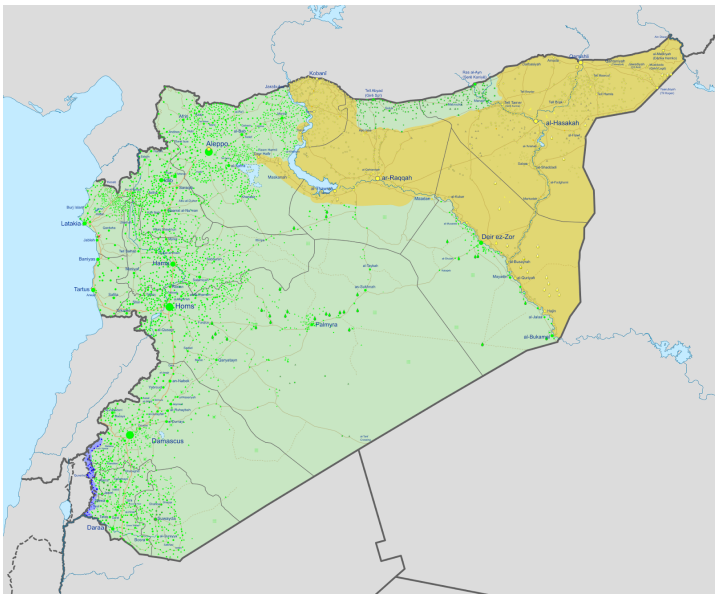
The ad hoc tribunals of the 1990s (for the former Yugoslavia and Rwanda) further developed individual criminal liability. These courts convicted military and political leaders for genocide, war crimes, and crimes against humanity. They established that superiors could be held responsible for subordinates' crimes under the doctrine of command responsibility. They also clarified that non-state actors could commit war crimes in non-international armed conflicts.[23]

The International Criminal Court, established by the Rome Statute in 2002, made individual criminal liability permanent. The ICC has jurisdiction over genocide, crimes against humanity, war crimes, and (since 2018) the crime of aggression. Importantly, it can prosecute individuals from non-state armed groups, not just state officials. The court has investigated situations involving groups from the Lord's Resistance Army in Uganda to various armed factions in the Central African Republic.[24]

But the ICC faces persistent challenges with non-state actors. Leaders of armed groups are rarely willing to surrender themselves. States hosting these groups may be unwilling or unable to arrest them. The court's investigations are slow, and by the time warrants are issued, suspects may be dead or disappeared. The Al Hassan conviction in 2024 took over a decade from when the crimes were committed.[25]

## Past Actions

The Rome Statute and ICC Jurisdiction: The ICC's founding treaty gives it jurisdiction over war crimes and crimes against humanity regardless of whether the perpetrator is a state official or non-state actor. Article 8 defines war crimes to include serious violations in both international and non-international armed conflicts. Article 25 establishes individual criminal responsibility for those who commit, order, or substantially contribute to such crimes.[26]




ICC Prosecutions of Non-State Actors: The court has actively pursued leaders of armed groups. Beyond the Al Hassan conviction, the ICC has issued warrants for leaders of the Lord's Resistance Army, the Sudanese Janjaweed militias, and various armed groups in the Central African Republic. In 2025, the court's prosecutor sought warrants for Taliban leaders for crimes against humanity, a landmark case focused on gender-based persecution.[27]

Ad Hoc and Hybrid Tribunals: When the ICC lacks jurisdiction or capacity, other mechanisms have filled gaps. The Special Court for Sierra Leone prosecuted leaders of armed factions in that country's civil war. The Extraordinary Chambers in the Courts of Cambodia addressed Khmer Rouge crimes. These models demonstrate how international and national justice can combine to address non-state actor crimes.[28]

Universal Jurisdiction: Some national courts claim jurisdiction over serious international crimes regardless of where they were committed. German courts have convicted Syrian officials for torture. French courts have tried individuals for Rwandan genocide. This "universal jurisdiction" provides an alternative pathway when international courts are unavailable, though it depends on suspects traveling to countries with such laws.[29]

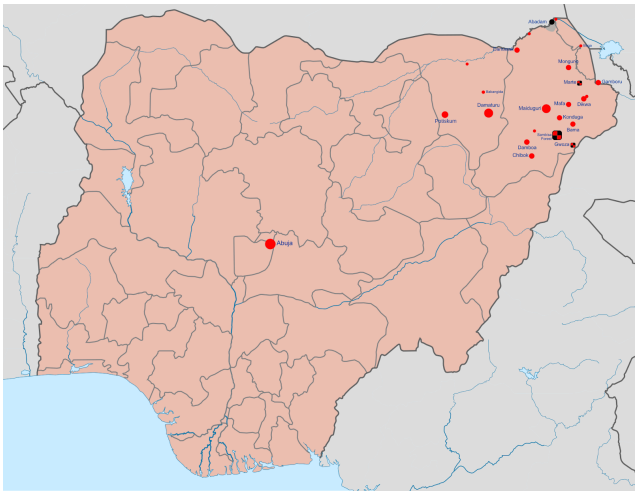
UN Security Council Referrals: The Security Council can refer situations to the ICC even when the relevant state isn't a Rome Statute party. This is how the ICC gained jurisdiction over Darfur (Sudan) and Libya. However, referrals require avoiding vetoes from permanent members, making them politically difficult for conflicts involving major power interests.[30]

## Possible Solutions

Strengthening ICC Enforcement: The ICC can issue warrants, but it can't arrest anyone; it depends entirely on states to do that. A treaty amendment could require Rome Statute parties to report on cooperation efforts and face consequences for failing to arrest suspects. Regional organizations could coordinate when suspects cross borders.

Clarifying Rules for Non-State Conflicts: The law of war for conflicts between states is detailed. For conflicts involving non-state groups, it's much thinner. An ILC study could clarify how international humanitarian law applies to modern armed groups, especially those that operate across borders or lack clear territorial control. Clearer rules would make prosecutions easier.

Hybrid Tribunals: When the ICC lacks jurisdiction or capacity, courts combining international and national elements can fill gaps. They can be established closer to where crimes happened, apply local law alongside international standards, and build domestic justice capacity. A standardized UN framework for creating such tribunals could make them easier to establish when needed.



## Potential Blocs

Understanding the major groupings in the Sixth Committee will help delegates find allies and anticipate debates.

NATO and Allied States: These countries have been frequent targets of state-sponsored cyberattacks and generally support strong rules on cyber operations. They've been developing their own legal positions on how international law applies to cyberspace. On accountability for non-state actors, they support the ICC but also use national courts and targeted sanctions.

Russia and China: Both countries are major cyber powers that resist efforts to constrain state behavior in cyberspace. They emphasize sovereignty and oppose what they see as Western dominance of international institutions. On the ICC,

neither is a Rome Statute party. Russia withdrew its signature after the court opened an investigation into the Crimea situation. China has never signed.

Non-Aligned Movement (NAM): This grouping of developing countries often emphasizes sovereignty and resists what they see as great-power dominance of international law. On cyber issues, they've pushed for more inclusive processes like the OEWG. On accountability, many support the ICC in principle but are wary of the court's focus on African situations.

Small and Vulnerable States: Countries most affected by cyber threats they can't defend against (from the Baltic states to small island nations) tend to support strong international rules and attribution mechanisms. On accountability, they generally support robust ICC jurisdiction and enforcement.

States Affected by Non-State Armed Groups: Countries actively fighting terrorist organizations or armed rebels have complex interests. They want international condemnation and potentially international prosecution of their enemies, but they may resist scrutiny of their own conduct in these conflicts.

ICC Member States: The 124 parties to the Rome Statute have committed to international criminal accountability and generally support strengthening the court's effectiveness. However, they differ on priorities and sometimes clash with the court over specific investigations.

# Glossary

Armed Attack — Under the UN Charter, an attack that triggers the right of self-defense. Whether cyberattacks can constitute "armed attacks" remains debated.

Attribution — The process of determining who is responsible for a cyberattack. Attribution is technically difficult and politically contested.

Command Responsibility — The legal doctrine holding military commanders responsible for war crimes committed by subordinates they failed to prevent or punish.

Common Article 3 — The provision appearing in all four Geneva Conventions that establishes minimum humanitarian protections in non-international armed conflicts.

Crimes Against Humanity — Widespread or systematic attacks against civilian populations, including murder, torture, and persecution. Can be committed in peace or war.

Cyber Operation — Any action using computer networks to access, degrade, or destroy information or systems. May range from espionage to destructive attacks.

Due Diligence — The obligation of states to prevent their territory from being used for operations harming other states, including by non-state actors.

International Criminal Court (ICC) — The permanent international court established in 2002 to prosecute genocide, crimes against humanity, war crimes, and aggression.

International Humanitarian Law (IHL) — The body of law governing the conduct of armed conflict, including protections for civilians and restrictions on weapons and tactics.

International Law Commission (ILC) — The UN body of legal experts tasked with progressively developing and codifying international law.

Non-International Armed Conflict — Armed conflict between a state and non-state armed groups, or between such groups, within a state's territory.

Non-State Armed Group — An organized armed force not part of a state's official military, including rebel groups, militias, and terrorist organizations.

Rome Statute — The 1998 treaty that established the International Criminal Court and defines its jurisdiction over international crimes.

State Responsibility — The legal principle that states are responsible for internationally wrongful acts, including those committed by their agents or those under their direction or control.

Tallinn Manual — An academic study of how international law applies to cyber operations, produced by experts at NATO's Cooperative Cyber Defence Centre of Excellence.

War Crimes — Serious violations of international humanitarian law in armed conflict, including attacks on civilians, torture of prisoners, and use of prohibited weapons.

# Footnotes


1. United Nations. "Sixth Committee (Legal)." UN General Assembly. https://www.un.org/en/ga/sixth/

2. International Law Commission. "About the Commission." United Nations. https://legal.un.org/ilc/

3. Wikipedia. "United Nations General Assembly Sixth Committee." https://en.wikipedia.org/wiki/United_Nations_General_Assembly_Sixth_Committee

4. Euromaidan Press. "Russian Cyberattacks on Ukraine Surge 70% in 2024 with 4,315 Assaults on Critical Infrastructure." January 2025. https://euromaidanpress.com/2025/01/12/russian-cyberattacks-on-ukraine-surge-70-in-2024/

5. CISA, FBI, NSA. "Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure." Joint Advisory, September 2024. https://media.defense.gov/2024/Sep/05/2003537870/-1/-1/0/CSA-Russian-Military-Cyber-Target-US-Global-CI.PDF

6. Just Security. "Cyberattack Attribution and International Law." https://www.justsecurity.org/71640/cyberattack-attribution-and-international-law/

7. NATO CCDCOE. "The Tallinn Manual." https://ccdcoe.org/research/tallinn-manual/

8. Cambridge University Press. "Tallinn Manual on the International Law Applicable to Cyber Warfare." 2013. https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/

9. Cambridge University Press. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." 2017. https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/

10. Trustwave. "The Russia-Ukraine Cyber War: Attacks on Critical Infrastructure." 2024. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-russia-ukraine-cyber-war-part-3/

11. UNODC. "United Nations Convention against Cybercrime." 2024. https://www.unodc.org/unodc/cybercrime/convention/home.html

12. University of Exeter. "Influential Resource on International Cyber Law Updated for 2024." News, 2024. https://news.exeter.ac.uk/influential-resource-on-international-cyber-law-updated-for-2024/

13. United Nations. "Open-Ended Working Group on Security of and in the Use of ICTs 2021-2025." https://www.un.org/disarmament/open-ended-working-group/

14. UN Press. "Speakers in First Committee Say Malicious Activity in Cyberspace Promotes Propaganda, Espionage, Disinformation." 2024. https://press.un.org/en/2024/gadis3749.doc.htm

15. Council of the European Union. "Cyberspace: Council Approves Declaration on Common Understanding of Application of International Law." November 2024. https://www.consilium.europa.eu/en/press/press-releases/2024/11/18/cyberspace-council-approves-declaration/

16. International Law Commission. "Articles on Responsibility of States for Internationally Wrongful Acts." 2001. https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

17. Institute for Economics & Peace. "Global Terrorism Index 2025." Vision of Humanity. https://www.visionofhumanity.org/maps/global-terrorism-index/

18. International Criminal Court. "Al Hassan Case: Trial Chamber X Pronounces Sentence." November 2024. https://www.icc-cpi.int/news/al-hassan-case-trial-chamber-x-pronounces-sentence

19. Council on Foreign Relations. "The Role of the ICC." Backgrounder. https://www.cfr.org/backgrounder/role-icc

20. Guide to International Humanitarian Law. "Non-International Armed Conflict (NIAC)." https://guide-humanitarian-law.org/content/article/3/non-international-armed-conflict-niac/

21. Nuremberg Trial Proceedings. "Judgment." International Military Tribunal, 1946.

22. ICRC. "Article 3 - Conflicts Not of an International Character." IHL Databases. https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/article-3

23. Guide to International Humanitarian Law. "Non-State Armed Groups." https://guide-humanitarian-law.org/content/article/3/non-state-armed-groups/

24. International Criminal Court. "About the Court." https://www.icc-cpi.int/about/the-court

25. International Bar Association. "International Criminal Court (ICC) Update – September 2024–March 2025." https://www.ibanet.org/International-Criminal-Court-September-2024-March-2025

26. Rome Statute of the International Criminal Court. Articles 8 and 25. https://www.icc-cpi.int/sites/default/files/2025-05/Rome-Statute-EN-2025.pdf

27. International Criminal Court. "Prosecutor Seeks Arrest Warrants for Taliban Leaders." January 2025. https://www.icc-cpi.int/news/

28. Coalition for the International Criminal Court. "Hybrid Tribunals." https://www.coalitionfortheicc.org/explore/hybrid-courts

29. Human Rights Watch. "Universal Jurisdiction." https://www.hrw.org/topic/international-justice/universal-jurisdiction

30. United Nations Security Council. "Referrals to the International Criminal Court." https://www.un.org/securitycouncil/content/referrals-international-criminal-court