International Journal of Cyber Law

# Sovereignty and Attribution Challenges in Modern State Cyber Warfare

**Javlonbek Omonboev**[1*]

[1] The Pennsylvania State University, USA
* *Javlonbekomonboev@gmail.com*

**ABSTRACT**

Cyber warfare increasingly challenges traditional sovereignty and attribution rules within international law. Existing legal frameworks remain territorially anchored, leaving hidden digital operations poorly addressed. This research examines how sovereignty doctrine and attribution standards intersect during modern state cyber conflict. It aims to identify gaps linking technical evidence to formal legal responsibility. The study uses a qualitative approach, applying doctrinal legal analysis and document review. Sources include treaties, judicial interpretations, and recent peer-reviewed scholarly literature. Results show attribution relies heavily on technical forensics rather than clear legal standards. Proxy actors weaken accountability, while treaties lack defined thresholds for armed attack. Deterrence weakens without reliable attribution, encouraging repeated cyber aggression across borders. Findings suggest combining evidentiary and legal frameworks could close these persistent gaps. Policymakers should invest in joint technical-legal institutions and clearer attribution standards today. This research concludes that sovereignty and accountability must be addressed together within evolving international cyber law.

**Keywords:** *Sovereignty, Attribution, Cyber Warfare, State Responsibility, Deterrence, Proxy Actors, International Law*

**HOW TO CITE THIS ARTICLE (APA 7th Edition)**

Omonboev, J. (2026). Sovereignty and Attribution Challenges in Modern State Cyber Warfare. *International Journal of Cyber Law*, *1*(2), 15–30. https://doi.org/10.59022/IRSHAD-iijcl.12

# I. INTRODUCTION

Cyber weapons now cross borders without ever crossing a physical line. A single attack can cripple a power grid Cyber weapons now cross borders without ever crossing a physical line. A single attack can cripple a power grid within seconds. States launch these operations while hiding behind screens and proxies. This creates a serious problem for international law today. Sovereignty once meant control over land, air, and sea. Now digital infrastructure sits inside that same protected national space. Attackers exploit this gap between old law and new modern war. Attribution becomes nearly impossible when evidence hides in code. Governments often deny responsibility even after strong technical evidence appears. Victim states struggle to respond without clear proof of source. This uncertainty weakens deterrence and encourages further cyber aggression. Legal scholars now debate how sovereignty applies to digital space. The question grows more urgent as state-sponsored attacks increase every single year. Understanding these challenges matters greatly for peace and lasting global security in every region of the world today (Ades, 2021).

State cyber conflict is not entirely new to legal thinking. Early scholars studied espionage and covert action between nations. But digital operations moved much faster than legal frameworks could adapt. Traditional laws of armed conflict assumed visible weapons and clear borders. Cyber operations instead use hidden code and rented digital infrastructure. This makes locating the true attacker extremely difficult for victim states. Researchers have examined how existing treaties apply to cyberspace. Yet most studies focus narrowly on technical detection methods alone. Fewer scholars connect attribution problems directly to sovereignty doctrine itself. This leaves a wide gap between technical proof and legal responsibility. Some studies discuss deterrence, while others discuss jurisdiction separately from each other. Rarely do they combine both issues within one coherent legal framework. This research addresses that gap by linking attribution and sovereignty together. It builds a clear picture of how cyber warfare challenges international law (Banks, 2021).

We already know that cyber attacks often hide their true origin. States use proxies, contractors, and anonymous networks to mask involvement. International law still lacks clear rules for these hidden operations. Existing legal frameworks focus mainly on state responsibility for direct military action. They rarely address indirect cyber operations run through private actors. This creates real confusion when courts try to assign clear legal blame. The specific problem is a mismatch between old rules and new modern tactics. Sovereignty protections assume a visible actor crossing a physical border. Cyber warfare removes that visibility, leaving victim states without clear legal remedies. What remains unclear is how attribution standards should adapt today. We still need much stronger legal tests connecting digital evidence to state responsibility. This research defines that missing link between digital proof and legal accountability. It clarifies exactly how sovereignty law must evolve for modern cyber threats worldwide (Buchan, 2016).

Early legal scholarship treated cyber warfare as a branch of traditional armed conflict. Dennis examined how existing laws of war might apply to digital attacks. This work mapped cyber operations onto rules built for physical battlefields. However, the analysis assumed attackers act openly, much like conventional armies do. Modern cyber operations rarely show themselves so clearly to victim states. This gap between assumption and reality weakens the framework's practical use today. Later scholarship shifted toward analyzing real-world cyber incidents for deeper insight. The Stuxnet case became a central example for testing legal boundaries. It showed how covert digital sabotage could bypass traditional attribution methods entirely. Findings revealed that legal categories built for war often fail here. Cyber operations sit awkwardly between espionage, sabotage, and open armed attack. This ambiguity leaves victim states uncertain about lawful response options available. Both studies highlight a persistent theme running across the literature (Dinniss, 2012).

Lindsay took a very different approach by studying the Stuxnet incident directly. He questioned whether Stuxnet truly represented a genuine form of cyber warfare. His analysis carefully compared Stuxnet against traditional legal definitions of armed attack. The findings clearly suggested cyber operations often produce limited strategic effects overall. This directly challenged earlier assumptions that cyber weapons could match physical warfare. Lindsay argued that raw technical complexity does not guarantee strategic success. His research exposed a wide gap between capability and actual battlefield outcomes. This finding matters greatly for sovereignty and attribution debates today. If effects remain limited, legal thresholds for armed attack become unclear. States may struggle to justify strong responses under existing legal standards. Both studies together reveal inconsistent thresholds across the wider literature. Scholars still disagree on when cyber operations cross legal red lines. This inconsistency creates the exact research gap this study seeks to close (Lindsay, 2013).

Existing literature builds strong theoretical models for cyber warfare and armed conflict. Yet these models rarely explain how sovereignty applies during covert operations. Dennis and Lindsay both focus heavily on legal classification of attacks. Neither study offers a practical test for confirming clear state responsibility. Attribution remains discussed mostly at a technical or forensic level only. Legal scholars have not fully connected forensic evidence to sovereignty claims. This clear gap appears when reviewing future research suggestions across many studies. Many scholars call for much stronger legal standards but rarely propose truly specific ones. Few works examine how courts might apply sovereignty doctrine to hidden actors. This research gap concerns the missing legal bridge between evidence and blame. Future research should build a workable framework linking both elements directly. Such a framework would guide states facing ambiguous digital attacks. It would also clarify when sovereignty violations trigger lawful countermeasures (AllahRakha, 2023).

To examine how existing sovereignty doctrine applies to covert state cyber operations.

To analyze current legal standards used for attributing cyber attacks to specific states.

To propose a clearer legal framework linking digital evidence to state responsibility under international law.

*How can international law establish a clear framework linking digital attribution evidence to state responsibility for sovereignty violations in covert cyber operations?*

This research holds clear value for both academic and practical audiences. Academically, it links two areas often studied separately in legal scholarship. Sovereignty doctrine and attribution standards rarely appear together within one coherent legal framework. This study fills that gap by connecting technical evidence directly to legal responsibility. Practically, states need clear legal tools for responding to modern cyber attacks today. Without such tools, victim states often hesitate before taking lawful action. This hesitation weakens deterrence and encourages further aggression across cyberspace. Policymakers can use this research to draft much stronger legal guidelines. Judges and legal practitioners also benefit from clearer attribution standards. Societal relevance grows as digital infrastructure becomes central to daily life. Citizens depend on stable systems that cyber attacks constantly threaten. This research therefore supports broader efforts toward global digital security. It offers a solid foundation for future scholarship in this evolving field (Prasad et al., 2025).

## II. METHODOLOGY

This research follows a qualitative research design suited for legal analysis. Qualitative methods allow deep examination of legal texts and scholarly arguments. This approach fits sovereignty and attribution questions better than numerical data. The research draws on international treaties, case law, and legal commentary. It also reviews national cyber laws, including regulations from Uzbekistan specifically. Uzbekistan's cyber security and data protection framework offers a useful example. This example illustrates how developing states approach sovereignty and attribution challenges. Keywords guiding source selection include sovereignty, attribution, cyber warfare, and armed attack. Additional keywords include state responsibility, deterrence, proxy actors, and humanitarian law. These keywords helped locate scholarly articles across major legal databases. Official government portals provided access to Uzbekistan's cyber security legislation. This combination of academic and official sources strengthens research credibility. Qualitative analysis therefore allows nuanced interpretation of complex, evolving legal concepts. This method suits research examining unsettled areas of international law well.

Data analysis relies primarily on doctrinal legal analysis and document review. Doctrinal analysis examines legal principles, treaty provisions, and judicial interpretations systematically. Document analysis involves close reading of statutes, policy papers, and academic articles. Both methods suit research questions centered on interpreting legal frameworks. Sources include recent scholarly articles, mostly published within the last five years. This timeframe ensures the research reflects currently applicable laws today. Older sources appear only when foundational to understanding doctrinal development. Validity depends on selecting peer-reviewed journal articles with clear scholarly credibility. Authors include established researchers, professors, and recognized legal experts internationally. Each source undergoes review for evidence support and appropriate citation practices. Uzbekistan's currently applicable cyber regulations were verified through official legislative portals. This verification ensures accuracy when discussing national legal frameworks. Reliability also depends on cross-referencing multiple sources addressing similar legal questions. This cross-referencing helps confirm consistency across different scholarly perspectives and interpretations.

This research uses only publicly available documents throughout this study. No private or confidential information was accessed at any stage. Every scholarly article referenced includes proper source citation in the text.

This practice honors the original authors whose ideas informed this analysis. The researcher declares no conflict of interest regarding this study. This research was conducted solely for academic and legal scholarship purposes. Delimitations include a focus on state sovereignty, attribution, and armed attack thresholds. The study does not address every possible cyber law topic. Uzbekistan serves as one illustrative jurisdiction rather than a full survey. Limitations include the evolving nature of technology and shifting policy landscapes. Cyber laws and regulations can change quickly, faster than scholarly publication. This creates a natural limitation regarding how current conclusions remain. Future research should revisit these findings as technology and policy continue evolving. Acknowledging these limitations strengthens transparency regarding the research's scope.

## III. RESULTS

This section presents the results addressing sovereignty and attribution in cyber warfare. The research question asked how international law can link digital evidence to responsibility. Each finding below connects directly to that central question and the stated objectives. Results move from doctrinal gaps toward practical legal solutions step by step. First, sovereignty doctrine still relies heavily on outdated territorial assumptions. Second, attribution processes remain divided between technical forensics and formal legal proof. Third, proxy actors complicate accountability by distancing states from direct blame. Fourth, treaties lack clear thresholds for classifying digital armed attacks properly. Fifth, weak deterrence follows naturally from these unresolved attribution problems. Together, these findings reveal a fragmented legal landscape needing structural reform. Military operations increasingly blur lines between covert action and open conflict. This blurring makes clear legal standards even more urgently necessary today. The following results build toward a coherent framework addressing these gaps (Mačák, 2021).

Sovereignty doctrine remains territorially anchored despite the rise of modern digital conflict. Traditional legal thinking ties sovereignty to land, air, and territorial waters. This narrow view fails to account for interconnected global digital networks today. Cyber infrastructure often spans multiple states through servers and data routes. Attacks can originate abroad while causing serious damage entirely within one territory. Current legal doctrine struggles to classify this cross-border digital harm clearly. Legal experts have tried extending traditional principles into cyberspace with mixed success. Some frameworks treat server locations as clear extensions of national territory itself. Others reject this approach, citing the borderless nature of digital networks. This unresolved debate leaves courts without a consistent standard to apply. States therefore interpret sovereignty violations differently, based on their own national interests. Such inconsistency undermines predictability within international cyber law overall. Modern warfare demands a much clearer definition that captures digital reality accurately (Schmitt, 2013).

Attribution relies heavily on technical forensics, not clear legal standards. Investigators trace digital attacks through code signatures and network paths carefully. This process identifies likely sources but rarely proves legal state responsibility. Courts and policymakers face a separate burden after technical findings emerge. They must translate forensic conclusions into recognized legal categories accurately. This translation step remains poorly defined within current international legal frameworks. Technical attribution offers probability, while international law demands a much higher evidentiary standard. This gap creates real uncertainty for states deciding exactly how to respond. Some experts strongly argue for one unified evidentiary threshold across both disciplines. Others firmly believe legal and technical processes should remain entirely separate always. This disagreement stalls the creation of consistent attribution rules worldwide today. Without unified standards, similar cyber incidents receive quite inconsistent legal treatment worldwide. States need much clearer guidance connecting forensic proof to formal legal responsibility (Schmitt, 2017).

Proxy actors significantly weaken state accountability under current sovereignty frameworks. States frequently rely on contractors, hackers, or loosely linked digital groups. This distancing strategy creates deniability while still achieving key strategic objectives. Existing attribution rules struggle to connect proxy actions clearly back to states. Legal tests often require solid proof of direct state control or instruction. Such proof rarely exists in covert digital operations conducted through hidden intermediaries. This evidentiary gap allows states to avoid formal legal responsibility rather easily. Scholars have strongly criticized this loophole as a serious flaw in doctrine. Some argue for lowering the strict control threshold applied to proxies. Others warn that lowering standards could unfairly implicate entirely uninvolved states. This tension remains largely unresolved within current sovereignty and attribution debates. Victim states clearly face delayed or blocked legal responses because of it. Closing this gap requires much clearer rules for proxy state responsibility (Spector, 2017).

Existing treaties offer no clear threshold for what counts as cyber armed attack. Traditional legal thresholds were built for visible, physical warfare scenarios only. Cyber operations rarely match these older categories in obvious or predictable ways. Some attacks cause serious economic harm without any physical destruction occurring. Legal frameworks struggle badly to classify such effects under armed attack rules. This creates real confusion about when digital harm justifies a forceful legal response. Recent legal scholarship calls for establishing clear normative thresholds specific to cyberspace. Digital borders now require distinct legal treatment from older physical territorial borders. Sovereignty protections must expand quickly to address this new normative gap. Without clear thresholds, states risk both overreaction and dangerous under reaction alike. Overreaction could escalate conflicts beyond their original digital scope entirely. Under reaction could embolden future attackers seeking similar strategic advantages. Establishing normative clarity remains essential for consistent international cyber governance today (Balarabe, 2025).

Deterrence weakens significantly without reliable and consistent attribution standards in place. States hesitate to respond firmly without solid legal footing behind them. This hesitation directly enables repeated cyber aggression across multiple jurisdictions worldwide. Attackers exploit this hesitation, knowing formal legal consequences rarely follow quickly. Weak deterrence creates a cycle where aggression grows increasingly bolder over time. Sovereignty itself becomes much harder to defend without predictable response mechanisms available. States need real confidence that lawful countermeasures will hold under close legal scrutiny. Without this confidence, many states simply absorb losses instead of responding. This pattern undermines the entire true purpose of sovereignty protections generally. Scholars argue that clearer legal thresholds could restore meaningful deterrence value. Predictable consequences would discourage states from launching covert digital operations. Restoring deterrence requires linking attribution evidence directly to legal consequences firmly. This connection remains the central challenge facing modern cyber warfare law (Corn & Taylor, 2017).

# IV. DISCUSSION

## A. Sovereignty Doctrine Remains Territorially Anchored

This finding answers part of the research question about outdated sovereignty limits. Sovereignty doctrine still assumes attacks cross a visible physical border. Digital operations rarely fit that older assumption in current legal practice today. This mismatch weakens legal protection for states facing hidden cyber threats. The importance here lies in closing gaps within current international legal frameworks. States cannot defend digital assets using rules built solely for physical territory. Supporting evidence shows courts struggling to classify server-based intrusions consistently. Legal scholars point to repeated disagreements over exactly what counts as sovereign space. This inconsistency directly supports the doctrinal gap identified earlier in this study. International cyber operations increasingly test these unsettled territorial boundaries. Recent legal commentary confirms that operations targeting infrastructure blur old distinctions. Without a redefined doctrine, states remain exposed to unresolved digital sovereignty claims. This finding therefore strengthens the case for expanding sovereignty beyond physical space (Delerue, 2020).

This finding carries strong significance for how states defend their own digital systems. It shows current sovereignty rules cannot fully protect national infrastructure alone. Collective defense arrangements have emerged partly to fill this clear legal gap. States now form partnerships to share threat information and coordinate responses. This shift reflects growing recognition that single-state doctrines are insufficient today. Key evidence comes from recent alliances built specifically around cyber defense cooperation. These arrangements extend protection well beyond narrow territorial sovereignty concepts alone. However, they also raise entirely new questions about collective legal responsibility. When multiple states respond jointly, attribution becomes even more complicated overall. This complexity connects directly back to the doctrinal gap discussed earlier here. Collective defense models offer partial solutions but not complete legal clarity. States must still resolve individual sovereignty questions before acting collectively. This finding highlights an emerging trend worth close scholarly attention going forward (Eichensehr, 2017).

Comparing recent incidents reveals how territorial doctrine performs under real world conditions. The Georgia-Russia conflict offers a very clear example of these legal tensions. Cyber operations there targeted government systems alongside conventional military action. This case shows sovereignty violations occurring across both physical and digital domains simultaneously. Legal analysis of that conflict exposed contradictions within existing attribution frameworks. Some experts classified the cyber component as a separate legal event. Others argued it formed part of one unified armed conflict entirely. This disagreement mirrors broader debates identified throughout

this current research study. It confirms that territorial doctrine struggles when digital and physical harm overlap. The case also highlights limitations in applying older legal categories consistently. Scholars still debate whether combined operations require entirely new legal tests. This contradiction strengthens the argument for doctrinal reform presented earlier. Real-world conflicts like this one demonstrate why clearer standards remain necessary (Gill & Tsagourias, 2015).

Several serious limitations affect how confidently this finding can be applied broadly. Sovereignty doctrine varies widely across legal systems and regional interpretations worldwide. This variation limits any single legal framework's ability to fit every single state. Bias may also arise from powerful states shaping legal interpretation themselves. Stronger states often heavily influence how tribunals define territorial sovereignty concepts. This influence can skew doctrine toward the interests of dominant global powers. Emerging technologies add further real complexity to these existing legal limitations. Artificial intelligence now plays a growing role in modern cyber operations design. Automated systems can launch attacks without any direct human decision-making involved. This development challenges assumptions built around deliberate direct state action alone. Sovereignty doctrine has not yet fully addressed autonomous digital operations. These gaps limit how completely current findings capture future scenarios. Researchers must remain cautious when generalizing across different technological contexts today (Achuthan et al., 2024).

Another important factor shaping this finding involves the rise of military artificial intelligence. States increasingly deploy automated tools for both offense and defense. This shift raises fresh questions about exactly who bears legal responsibility for outcomes. When machines act independently, tracing state control becomes far more difficult. Sovereignty doctrine assumes human decision-makers direct state action deliberately. Artificial intelligence disrupts this assumption by acting without constant human oversight. This factor influences attribution debates discussed throughout earlier sections of this current research. It also complicates efforts to apply territorial sovereignty to autonomous digital operations. Military planners must now consider legal exposure from automated system failures. States deploying these tools face uncertain liability under current international legal standards. This uncertainty adds another layer to the territorial doctrine problem identified earlier. Addressing artificial intelligence directly within sovereignty frameworks appears increasingly necessary. This factor cannot be separated from broader attribution and sovereignty debates (Boutin, 2023).

This finding carries broad implications for how states classify future cyber operations. Territorial doctrine can no longer stand alone as the primary legal test. States need frameworks accounting for digital and physical harm together. This applies directly to policy discussions currently shaping cyber governance today. Recent efforts to define cyber operations reflect this exact shifting legal reality. Scholars now propose broader definitions covering intent, effect, and digital reach together. These proposals move away from purely territorial thinking toward functional analysis. Applying these ideas could resolve inconsistencies identified earlier in this study. States adopting broader definitions gain clearer legal grounds for responding firmly. This approach also supports better coordination between military and legal decision-makers. Practical applicability depends on states actually adopting these updated legal definitions. Without adoption, sovereignty doctrine risks remaining outdated despite growing scholarly consensus. This finding points directly toward necessary reform across international cyber law (Ducheine & Pijpers, 2021).

## B. Attribution Relies on Technical Forensics, not Legal Standards

This finding answers how attribution actually works in modern cyber conflicts. Investigators identify attackers through digital fingerprints, not formal legal proof. States often announce findings publicly before any legal process begins. This public naming shapes political reactions more than legal consequences. The importance here lies in exposing a serious accountability gap. Technical confidence does not automatically translate into legal state responsibility. Public attribution frameworks now guide how governments announce cyber attackers. These frameworks focus on credibility, timing, and diplomatic messaging strategies. They rarely reference formal legal thresholds required under international law. This creates a widening gap between political statements and legal accountability. Recent government announcements often cite technical evidence without citing any formal legal standards. This pattern strengthens the earlier argument about fragmented attribution processes. Understanding this distinction matters greatly for future international policy design. Clearer integration between technical and legal standards remains urgently needed today (Egloff & Smeets, 2023).

This finding carries weight for armed attack classification rules. Legal scholars debate whether technical attribution can satisfy armed attack tests. International law demands rigorous proof before authorizing forceful response. Technical evidence alone rarely meets this demanding evidentiary threshold consistently. This mismatch

directly threatens victim states seeking lawful countermeasure options. Key evidence shows states hesitating despite having strong technical attribution reports. Legal experts note that armed attack classification requires more than mere suspicion. This requirement protects against wrongful accusations but also delays needed responses. The tension between speed and legal certainty remains largely unresolved. This connects directly to the earlier finding about technical versus legal proof. Some scholars propose lowering evidentiary thresholds specifically for cyber incidents. Others warn this could weaken protections against false attribution claims. This disagreement highlights the ongoing struggle to harmonize both standards. Resolving this tension remains central to advancing meaningful cyber accountability today (Finlay & Payne, 2019).

Comparing recent scholarship reveals fresh tension around artificial intelligence and attribution. Some experts argue new technology could improve attribution accuracy significantly. Machine learning tools now analyze malware patterns faster than human investigators. This capability strengthens technical confidence in identifying likely attack sources. However, faster technical results do not automatically resolve legal uncertainty. Legal standards remain unchanged despite advances in detection technology speed. This contradiction highlights a growing gap between technical progress and legal reform. Scholars note that international law struggles to keep pace with innovation. Some propose updating legal frameworks to address artificial intelligence attribution. Others argue existing frameworks remain flexible without major structural changes. This disagreement reflects broader tension identified throughout earlier sections of this study. Faster technical tools alone cannot substitute for missing legal clarity. The contradiction reinforces why combining both disciplines remains essential going forward. Real progress requires aligning technological capability with formal legal accountability (Ghannadi, 2025).

This finding carries clear limitations worth acknowledging before drawing broad conclusions. Attribution symposium discussions often reflect Western legal traditions and priorities. This narrow scope may overlook perspectives from other legal systems worldwide. Bias may also exist within technical attribution methods themselves today. Companies conducting forensic analysis sometimes have commercial or political interests involved. These interests can shape how confidently attackers get publicly named. Symposium contributors acknowledge these challenges but rarely resolve them fully. This creates real uncertainty around how neutral attribution processes truly remain. Weapon systems now embed complex digital components requiring specialized technical review. These systems raise fresh questions about attribution when malfunctions occur unexpectedly. Standards for reviewing such systems remain inconsistent across different states. This inconsistency limits how completely current attribution methods apply universally. Researchers should approach generalizations here with appropriate caution and nuance. Future studies must address these limitations more directly and much more thoroughly (Hakimi, 2019).

Another factor shaping this finding involves growing cyber security requirements for weapon systems. Modern militaries increasingly rely on digitally connected weapon platforms today. These platforms face constant risk from hostile cyber intrusion attempts. Technical standards now guide how militaries secure these sensitive systems. However, international legal requirements for weapon system cyber security remain relatively underdeveloped. This gap complicates attribution when weapon systems experience unexplained failures. Investigators must determine whether failures resulted from cyber attacks or malfunctions. This determination requires close cooperation between engineers and legal experts. Current frameworks rarely mandate this cooperation formally or consistently. This factor connects directly to earlier findings about fragmented attribution processes. Weapon system vulnerabilities add urgency to resolving these technical-legal gaps. States face growing pressure to secure systems while maintaining legal accountability. This factor cannot be separated from broader attribution and sovereignty debates. Addressing it directly remains essential for advancing meaningful cyber governance (Kajander et al., 2025).

This finding carries clear implications for how states approach cyber policy. Attribution reform requires coordinated action between technical and legal communities. European institutions have begun addressing this gap through strategic policy initiatives. Recent discussions highlight persistent gaps in cyber conflict governance below war thresholds. This vacuum leaves states without clear guidance for responding to low-level incidents. Applying these insights could help build stronger regional attribution frameworks. States adopting coordinated approaches gain clearer grounds for justified responses. This approach also supports better alignment between technical evidence and legal action. Practical applicability depends on states actively investing in joint frameworks. Without investment, attribution processes will remain fragmented and inconsistent globally. This finding supports the broader argument made throughout this research. Combining technical accuracy with legal clarity strengthens overall cyber accountability. Policymakers should treat this combination as a genuine priority now. Sustained cooperation remains essential for closing this persistent legal gap (Liebetrau, 2022).

## C. Proxy Actors Weaken State Accountability

This finding answers how proxy relationships weaken state accountability under law. States often distance themselves from operations run through hackers or contractors. This tactic exploits gaps in existing legal attribution methods. The importance here lies in exposing a deliberate accountability loophole. Proxy use lets states pursue aggressive goals while avoiding formal blame. Supporting evidence shows deep technical analysis rarely produces clear legal outcomes. Investigators can trace malware to specific groups with reasonable confidence. Yet linking those groups formally to state control remains extremely difficult. This gap between technical tracing and legal proof repeats throughout cyber law. Recent incidents confirm states increasingly rely on this proxy strategy. Analysts note growing sophistication in disguising direct state involvement. This sophistication makes proxy relationships much harder to expose through evidence. Understanding this pattern matters for improving future accountability frameworks. Closing this gap requires rethinking how the control standards apply legally (Rid & Buchanan, 2015).

This finding matters for negotiations shaping future cyber governance rules. Some states push to redefine sovereignty in ways favoring state control. United Nations negotiations reveal this tension between competing legal visions. Certain states argue for stronger territorial control over digital networks. This position could reduce reliance on proxy actors within their borders. However, it also risks legitimizing greater state surveillance and restriction. Key evidence shows negotiations remain deeply divided along competing interests. Some states favor open, liberal frameworks resisting territorial restrictions entirely. Others push firmly toward state-centered control over domestic cyber activity. This split directly affects how proxy accountability rules might eventually develop. Stronger state control could reduce proxy use but increase censorship risks. Weaker control could preserve openness but sustain existing accountability gaps. This tension reflects broader disagreements identified throughout earlier sections of this study. Resolving it requires balancing accountability against fundamental digital freedoms carefully (Sukumar & Basu, 2024).

Comparing legal interpretations under the United Nations Charter reveals further contradictions. Some scholars argue sovereignty violations require significant physical or economic harm. Others believe any unauthorized digital intrusion already violates territorial sovereignty rights. This disagreement matters directly for how proxy operations get classified legally. If harm thresholds stay high, many proxy attacks escape formal violation status. If thresholds lower, more incidents could trigger legal state responsibility. Recent charter-based analysis highlights this unresolved interpretive divide clearly. Some tribunals lean toward stricter harm requirements before finding violations. Other scholars argue this strictness protects states using proxies deliberately. This contradiction connects directly to the earlier finding about accountability loopholes. Lower thresholds could close gaps but risk excessive legal intervention. Higher thresholds protect state sovereignty but weaken victim state protections. This ongoing debate shows no clear consensus currently exists among legal scholars. Charter interpretation therefore remains central to resolving proxy accountability questions (Assaf, 2023).

This finding carries important limitations affecting how broadly conclusions can apply. International attribution law remains slow to develop meaningful, binding rules. Scholarly commentary often outpaces actual state practice by considerable margins. This gap between theory and practice limits real-world applicability of proposals. Bias may exist because scholars often write from within powerful states. Their perspectives may unintentionally favor frameworks benefiting their own governments. Smaller states rarely shape these academic debates to the same degree. This imbalance limits how representative current attribution scholarship truly remains. Legal commentary also tends to focus heavily on high-profile incidents only. Smaller, less publicized proxy operations receive far less scholarly attention. This selective focus may distort perceptions of how common proxy tactics really are. Researchers should treat current findings as partial rather than complete. Future work must examine underrepresented states and lower-profile incidents thoroughly. Broader inclusion would strengthen confidence in attribution law conclusions overall (Banks, 2019).

Another factor influencing this finding involves domestic political discourse within states. National parliaments increasingly debate cyber sovereignty within their own legislative processes. These debates shape how states approach international attribution obligations later. Lawmakers often frame cyber sovereignty through national security priorities first. This framing can push states toward protective, defensive legal positions instead. Such positions sometimes conflict with international efforts toward shared accountability standards. Domestic political pressure can therefore complicate international attribution cooperation significantly. States facing strong nationalist rhetoric may resist external oversight mechanisms. This factor connects directly to earlier findings about fragmented global approaches. Parliamentary discourse also reveals how sovereignty debates now shape everyday policymaking. Politicians increasingly reference cyber threats when justifying new legislative measures. This trend influences how proxy accountability gets addressed domestically over time. Recognizing this factor helps explain why international

consensus remains elusive. Domestic politics and international law must eventually align for real progress (Beisenbayev, 2026).

This finding carries broad implications for how states manage intelligence-linked cyber operations. Much proxy activity overlaps directly with state intelligence gathering functions. Intelligence operations traditionally remain shielded from public legal scrutiny entirely. This secrecy makes proxy accountability even harder to achieve meaningfully. Breaking this silence could improve transparency around state-sponsored cyber activity. Some policymakers now call for limited diplomatic disclosure of intelligence operations. Such disclosure could help distinguish legitimate intelligence work from unlawful proxy attacks. This distinction matters greatly for applying accountability standards fairly and consistently. Applying these ideas requires balancing national security against transparency needs carefully. States adopting limited disclosure practices could strengthen international trust gradually. Practical applicability depends on states accepting some loss of operational secrecy. Without this shift, proxy accountability gaps will likely persist indefinitely. This finding reinforces the broader argument made throughout this research. Breaking diplomatic silence remains essential for advancing genuine cyber accountability (Broeders, 2024).

## D. Existing Treaties Offer No Clear Threshold for Cyber Armed Attack

This finding answers why current treaties fail to define cyber armed attack. Existing frameworks were drafted before digital warfare became a serious concern. They focus heavily on state actors while largely ignoring non-state involvement. Non-state actors now play a growing role in modern cyber conflict. This gap creates real legal uncertainty when private groups launch attacks. The importance here lies in exposing how outdated treaties fail today. Without clear thresholds, states struggle to justify lawful defensive action. Supporting evidence shows scholars pushing for updated international frameworks specifically. These frameworks aim to address non-state actors directly and clearly. Current proposals suggest expanding legal definitions beyond traditional state-only categories. This expansion could help close existing thresholds gaps meaningfully. Recent academic work highlights growing urgency around this specific issue. Legal reform efforts remain slow despite widespread scholarly agreement on need. Addressing this gap requires coordinated international treaty negotiation moving forward (Di Scipio, 2021).

This finding holds real significance for how complicity gets treated legally. States sometimes assist others in launching offensive cyber operations indirectly. Current law offers little clarity on complicity thresholds for such assistance. This gap matters because complicity differs legally from direct state action. A state providing tools or intelligence may still avoid formal blame. Key evidence shows scholars debating what level of assistance triggers responsibility. Some argue mere technical support should trigger meaningful legal consequences. Others believe only active operational involvement should count as complicity. This disagreement directly affects how armed attack thresholds get applied. Without clear complicity standards, indirect state involvement remains largely unaddressed. Recent conference discussions highlight growing scholarly interest in this specific issue. Experts increasingly call for codifying complicity rules within cyber warfare law. This significance connects directly to the earlier finding about treaty gaps. Addressing complicity remains essential for closing existing armed attack loopholes (Haataja, 2023).

Comparing regional experiences reveals how thresholds apply unevenly across different states. South African cyber incidents highlight gaps facing developing nations specifically. These states often lack resources for advanced technical attribution capabilities. Weaker technical capacity makes proving armed attack thresholds much harder. This creates a real geopolitical imbalance within existing international legal frameworks. Wealthier states can more easily meet demanding armed attack thresholds. Developing states struggle to gather sufficient evidence for similar claims. This contradiction directly challenges assumptions of equal treatment under international law. Recent regional analysis confirms these disparities remain largely unaddressed globally today. Some scholars argue thresholds should account for varying technical capacity. Others insist uniform standards must apply regardless of national resources. This disagreement mirrors broader tension identified throughout earlier sections of this study. Regional case studies like this one expose real-world consequences of ambiguity. Addressing these disparities requires considering capacity alongside legal threshold design (Henrico, 2025).

This finding carries clear limitations regarding how policymakers can apply it. Decision-taking frameworks for retaliation remain largely theoretical rather than operational. Few states have publicly tested these frameworks during actual incidents. This limits confidence in how well proposed models perform under pressure. Bias may also exist since most frameworks come from academic settings. Real political and military constraints often shape decisions differently than theory suggests. Policymakers face pressure from public opinion, alliances, and diplomatic relationships. These pressures rarely appear within clean, academic decision-making models. This gap between theory and practice weakens direct real-world applicability. Existing frameworks also assume rational, consistent state

behavior throughout crisis situations. Actual state responses often involve confusion, delay, and competing internal interests. This limitation echoes earlier concerns about gaps between scholarship and practice. Researchers should treat these frameworks as starting points, not final solutions. Testing them against real incidents remains necessary for validating usefulness (Leventopoulos, 2024).

Another factor shaping this finding involves the practical feasibility of cyber deterrence. Deterrence theory assumes attackers fear identifiable, credible legal or military consequences. Without clear attribution, deterrence loses much of its intended power. This connects directly to the earlier finding about undefined armed attack thresholds. States cannot deter attacks they cannot confidently and consistently attribute. This weakness influences how aggressively states pursue attribution capabilities today. Some governments now invest heavily in improving attribution technology and speed. Faster attribution could theoretically restore some deterrent effect over time. However, speed alone cannot replace missing legal threshold clarity entirely. This factor highlights how technical and legal solutions must work together. Deterrence remains incomplete without both reliable attribution and defined thresholds. This combination directly supports the broader argument developed throughout this research. Recognizing this factor helps explain persistent hesitation among many victim states. Strengthening deterrence requires addressing both technical and legal dimensions (Lindsay, 2015).

This finding carries implications for regional and international policy development. The European Union now actively debates digital sovereignty within policy discussions. These discussions increasingly touch on cyber defense and armed attack thresholds. Applying insights from this research could strengthen European legal coordination. States adopting shared threshold definitions gain clearer grounds for collective response. This approach also supports stronger alignment between member states facing similar threats. Practical applicability depends on political will to accept binding regional standards. Without such commitment, thresholds will likely remain vague and inconsistent regionally. This finding reinforces the broader argument developed throughout this research. Combining regional cooperation with clearer definitions strengthens overall cyber accountability. Policymakers should treat threshold clarity as a genuine, urgent priority. The European experience offers useful lessons for other regional cyber initiatives. Sustained political commitment remains essential for closing this persistent legal gap. Wider adoption elsewhere could accelerate meaningful legal reform globally (Hulkó, 2025).

## E. Deterrence Weakens without Reliable Attribution Standards

This finding answers how weak attribution directly undermines meaningful deterrence value. States cannot punish attackers they cannot confidently identify beforehand. This uncertainty encourages repeated aggression against poorly defended digital targets. The Solar Winds incident illustrates this problem clearly on a global scale. Attackers penetrated numerous government and corporate networks undetected for many months. Investigators eventually traced the intrusion but faced significant attribution delays. This delay weakened any meaningful deterrent response during the critical period. The importance here lies in clearly showing how attribution speed affects outcomes. Slow attribution allows attackers to operate freely before real consequences arrive. Humanitarian organizations also faced disruption from this widespread cyber intrusion. This case demonstrates real-world consequences beyond typical government targets alone. Weak deterrence therefore threatens both state and civilian digital infrastructure equally. Understanding this connection matters greatly for future defensive policy design. Strengthening attribution speed remains essential for restoring credible deterrent powerfully (Marelli, 2022).

This finding matters for how digital sovereignty relates to deterrence capability. Sovereignty debates increasingly connect infrastructure control to national security strategy. States argue that controlling digital networks strengthens defensive capabilities directly. This connection reveals sovereignty as more than symbolic territorial protection. Key evidence shows growing policy focus on digital infrastructure independence globally. Governments now invest heavily in domestic technology and network sovereignty projects. This trend reflects concern over foreign influence within critical digital systems. Sovereignty and deterrence therefore increasingly overlap within modern security thinking. States with stronger digital sovereignty may better detect and attribute attacks. This connection supports earlier findings linking attribution weakness to reduced deterrence. However, sovereignty-focused policies also risk fragmenting global cyber cooperation efforts. Excessive control could isolate states from shared threat intelligence networks. This tension highlights complexity within current digital sovereignty policy debates. Balancing independence with cooperation remains essential for effective deterrence strategy (Pohle & Thiel, 2020).

Comparing artificial intelligence policy debates reveals fresh contradictions within sovereignty thinking. Some scholars argue artificial intelligence strengthens state control over digital defense. Others warn it introduces new vulnerabilities that weaken sovereign security instead. This contradiction directly affects how deterrence strategies

incorporate emerging technology. Automated systems could theoretically speed up attribution and improve response times. Yet automated systems also create new attack surfaces for adversaries. This dual nature complicates simple assumptions about technology strengthening deterrence. Normative approaches now call for careful, ethical integration of artificial intelligence. These approaches emphasize accountability alongside technological advancement within security systems. Without such accountability, automated defense tools could produce unreliable attribution outcomes. This risk connects directly to earlier findings about attribution weakening deterrence. Scholars remain divided over how quickly states should adopt these tools. Some urge caution, while others push for rapid technological integration. This ongoing contradiction shapes how future deterrence strategies will evolve (Roberts, 2024).

This finding carries limitations regarding how broadly conclusions apply globally. Data policy debates around platforms like TikTok reveal cultural and political differences. Different states interpret cyber sovereignty according to their political priorities. This variation limits how universally attribution and deterrence lessons transfer. Bias may exist because dominant narratives often reflect Western security concerns. Non-Western states sometimes prioritize economic control over security objectives instead. This difference complicates assumptions about shared deterrence goals across all states. Comparative studies show sovereignty concepts differ significantly between political systems. Some states emphasize data localization more than attribution capability itself. This divergence limits how consistently deterrence frameworks apply internationally today. Researchers must remain cautious about generalizing findings across diverse political contexts. Cultural and political factors shape sovereignty debates as much as security concerns. This limitation echoes earlier concerns about uneven global capacity and interpretation. Future research should incorporate broader comparative perspectives beyond dominant narratives (Su, 2023).

Another factor shaping this finding involves how philosophy influences modern deterrence thinking. Classical just war theory now informs debates about legitimate cyber response. Scholars draw on historical thinkers to justify distributed deterrence approaches. This philosophical grounding shapes how policymakers frame acceptable countermeasure options. Distributed deterrence involves both public institutions and private sector cooperation. Private companies increasingly play defensive roles alongside government agencies. This shift reflects growing recognition that states alone cannot ensure security. Philosophical justifications help legitimize this expanded, shared responsibility model publicly. This factor connects directly to earlier findings about fragmented attribution processes. Distributing responsibility could improve detection speed across wider digital networks. However, it also raises questions about accountability when private actors respond. This complexity mirrors broader tensions identified throughout earlier sections of this study. Recognizing philosophical influences helps explain evolving deterrence strategy justifications today. Balancing public and private roles remains central to future deterrence design (Thumfart, 2020).

This finding carries direct implications for how self-defense law applies practically. Legal debates around cyber self-defense remain closely tied to attribution problems. States hesitate to invoke self-defense without confident, verified attribution evidence. Applying insights from earlier findings could strengthen legal justifications for response. Clearer attribution standards would give states firmer legal grounds for action. This approach also supports more consistent application of self-defense doctrine. Practical applicability depends on states investing in faster attribution capabilities. Without such investment, self-defense claims will remain legally vulnerable and contested. This finding reinforces the broader argument developed throughout this entire research. Combining reliable attribution with clear legal standards strengthens overall deterrence power. Policymakers should treat attribution investment as a genuine security priority. Legal scholars continue debating how self-defense thresholds should adapt today. Sustained attention to attribution remains essential for closing this persistent gap. Progress here would meaningfully strengthen deterrence across future cyber conflicts (Tsagourias, 2012).

## F. A Combined Evidentiary-Legal Framework Can Close the Identified Gap

This finding answers how combining evidence with law closes existing gaps. Technical proof alone cannot establish formal state legal responsibility. Legal standards alone cannot verify who launched an attack. Together, these tools create a stronger, reliable accountability system. The importance here lies in bridging two disconnected disciplines. States need both technical confidence and legal certainty first. Supporting evidence shows growing calls for integrated attribution and legal review. Some governments now pair technical teams with legal advisors directly. This pairing helps translate forensic findings into recognized legal claims. Recent policy discussions increasingly favor this combined institutional approach. Analysts argue this model reduces both false accusations and missed responses. It also strengthens confidence when states pursue formal countermeasures publicly. This finding connects directly to

earlier gaps identified throughout this research. A combined framework offers a clear path toward reform. Building this framework requires sustained cooperation across technical and legal fields (Carpenter, 2025).

This finding carries broad significance for how emerging digital domains get governed. New spaces like the met averse now raise fresh sovereignty questions entirely. States must decide whether existing frameworks extend into these new environments. This decision affects how future attribution and accountability rules develop. Key evidence shows countries taking sharply different regulatory approaches already. Some states favor open, permissive policies encouraging rapid digital expansion. Others push for strict, sovereignty-focused control over emerging digital spaces. This split reflects broader disagreements identified throughout earlier sections of this research. Combined evidentiary-legal frameworks could help harmonize these divergent regulatory paths. Clear standards would help states apply attribution rules consistently across domains. Without harmonization, emerging digital spaces risk repeating existing attribution problems. This significance connects directly to concerns about cross-border accountability gaps. Policymakers must consider these new domains when designing combined frameworks today. Ignoring them risks creating fresh gaps even as old ones close (Zhang, 2025).

Comparing recent joint attribution efforts reveals both promise and unresolved tension. Some states now coordinate publicly to name attackers together formally. This collective approach strengthens credibility compared to single-state accusations alone. Joint attribution combines multiple separate technical assessments into one clear unified conclusion. This process could support the combined framework proposed throughout this research. However, coordinating several states also creates new procedural complications entirely. Different states may weigh evidence differently before reaching final conclusions. This disagreement can delay joint announcements despite growing political pressure. Some scholars argue joint attribution strengthens legal legitimacy significantly overall. Others worry it dilutes individual state accountability within larger coalitions. This contradiction mirrors broader tension identified throughout earlier sections of this study. Joint efforts show real promise but require much clearer internal coordination rules. Building formal joint attribution frameworks could accelerate broader accountability reform efforts. This comparison highlights both opportunity and remaining procedural challenges ahead (AllahRakha, 2023).

This proposed combined framework carries important limitations worth acknowledging honestly here. Building shared standards requires cooperation between states with quite differing legal traditions. This diversity makes universal agreement difficult to achieve quickly. Bias may also arise since powerful states could dominate framework design. Their interests might shape rules in ways favoring their own capabilities. Smaller states could struggle to influence combined framework negotiations equally. This imbalance limits how representative any resulting framework truly becomes. Institutional cooperation also requires significant resources many states currently lack. Developing nations may struggle to participate fully in complex negotiations. This resource gap limits how inclusive framework development processes remain overall. Cross-national policy comparisons reveal similar imbalances across other digital governance efforts. These patterns suggest similar challenges likely await combined attribution frameworks too. Researchers should acknowledge these structural limitations when proposing new solutions. Addressing resource and representation gaps remains necessary for meaningful lasting reform (Pierucci, 2025).

Another factor influencing this finding involves recent conflicts testing these ideas. The Israel-Iran conflict showed cyber operations paired closely with physical military action. This pairing illustrates how combined frameworks might apply during hostilities. Analysts tracked cyber intrusions alongside precision military strikes throughout the conflict. This combination challenges purely technical or purely legal analysis alone. A joint framework proved more useful for understanding overall conflict dynamics. This factor connects directly to earlier findings about fragmented attribution processes. Real conflicts demonstrate why combined approaches matter beyond theoretical discussion. Military planners increasingly consider cyber and physical operations as interconnected tools. This shift reflects growing recognition that modern warfare rarely stays separate. Recognizing this factor helps explain growing urgency behind combined framework proposals. Recent events validate the practical relevance of this research direction. Continued attention to conflicts remains essential for refining frameworks. Real-world testing offers valuable lessons for future combined framework design (Popalzay, 2025).

This finding carries implications for how states should design future policy. A combined evidentiary-legal framework offers a practical path toward closing gaps. Applying insights from earlier findings could strengthen technical and legal cooperation. States adopting combined approaches gain clearer grounds for justified responses. This approach also supports better alignment between forensic evidence and formal law. Practical applicability depends on states investing jointly in shared institutional structures. Without investment, technical and legal processes will likely remain separate indefinitely. This finding reinforces the broader argument developed throughout this research. Combining technical accuracy with legal clarity strengthens cyber accountability. Policymakers should treat

this combination as a genuine, urgent priority now. Institutions must support ongoing dialogue between technical and legal communities. Sustained cooperation remains essential for closing this persistent evidentiary-legal gap. Progress here would meaningfully strengthen accountability across future cyber conflicts. This research points toward a clear, actionable path forward (Hidalgo et al., 2024).

### G. Implication

This research challenges the assumption that territorial sovereignty alone can govern digital conflict. It shows that attribution and accountability require combined technical and legal analysis together. Existing theories built around visible, physical armed attack no longer fit hidden cyber operations well. This shift demands updated legal thinking beyond traditional state-centered frameworks entirely. Positive outcomes include clearer accountability paths and stronger deterrence against future cyber aggression. Negative outcomes include possible overreach if lower thresholds encourage hasty, premature state responses instead. Legal frameworks currently struggle with proxy actors, weapon system failures, and undefined armed attack limits. Policymakers could apply these findings by building joint technical-legal review institutions within their own governments. Judges could apply clearer evidentiary standards when evaluating state responsibility claims formally. Victim states, smaller nations, and international courts would benefit most from this clarity. Real-world applications include treaty reform, coordinated attribution announcements, and updated military cyber policy guidance. Recent conflicts, including Israel-Iran cyber operations, clearly show why reform matters urgently and practically today. Limitations remain, since political will and resource gaps could slow meaningful adoption significantly. Despite these constraints, this research offers a workable path toward stronger sovereignty and attribution standards for future international cyber governance efforts across the world.

## CONCLUSION

Modern warfare now unfolds across invisible digital networks rather than open battlefields. States launch attacks through hidden code, proxies, and disguised digital operations. This shift challenges sovereignty and accountability rules built for physical conflict decades ago. Understanding how law responds to these hidden threats matters greatly today. Digital infrastructure now underpins hospitals, banks, governments, and everyday civilian life. A single unattributed attack can disrupt entire societies without any warning. This research examined how sovereignty doctrine and attribution standards intersect within cyber warfare. It asked how international law could better connect evidence to responsibility. Answering this question matters far beyond academic legal debate alone. Governments, courts, and international institutions all face these unresolved questions daily. Cyber conflict now shapes diplomatic relations, military strategy, and national security policy. Recent incidents involving major infrastructure and regional conflicts confirm growing urgency. This broader context shows why closing legal gaps remains a pressing global priority.

Several key patterns emerged throughout this research, each reinforcing one central argument. Sovereignty doctrine still relies heavily on outdated, purely territorial assumptions. This reliance leaves states poorly equipped to address hidden digital intrusions effectively. Attribution processes remain divided between technical forensics and formal legal proof. Investigators can trace attackers technically, yet courts demand a separate legal standard. This gap weakens deterrence and encourages states to avoid formal accountability entirely. Proxy actors deepen this problem by distancing states from direct legal blame. Together, these patterns reveal a fragmented legal system struggling against modern threats. Combining technical evidence with clearer legal standards could close this persistent gap. Recent efforts toward joint public attribution show growing recognition of this need. These connected findings strengthen the argument that reform cannot happen piecemeal. Sovereignty, attribution, and accountability must be addressed together, not separately. This integrated understanding forms the strongest basis for meaningful legal progress ahead.

These findings carry meaningful weight for how states design future cyber policy. Governments could apply combined evidentiary-legal frameworks when responding to hidden digital threats. Courts could rely on clearer standards when evaluating state responsibility claims formally. International institutions could use these insights to guide treaty reform discussions. Recent regional initiatives, including European digital sovereignty debates, already reflect this direction. Smaller states and victim nations stand to benefit most from clearer rules. They currently face the greatest disadvantage when confronting well-resourced, hidden attackers. Practical steps could include joint technical-legal review bodies within national governments. Future research should examine how artificial intelligence reshapes attribution and accountability further. Scholars should also study how developing nations can participate more fully. Questions remain about balancing transparency with legitimate national security concerns carefully.

Continued attention to these questions will help legal frameworks keep pace. Progress here would strengthen global stability across an increasingly connected digital world.

# BIBLIOGRAPHY


Achuthan, K., et al. (2024). Advancing cybersecurity and privacy with artificial intelligence. In *International Conference on Cyber Warfare, Security and Space Research* (pp. 130–143). Springer. https://doi.org/10.1007/978-3-031-15784-4_11

Ades, P. A. (2021). Why international law and norms do little in preventing non-state cyber operations. *Journal of Cybersecurity, 7*(1), tyab009. https://doi.org/10.1093/cybsec/tyab009

AllahRakha, N. (2023). Cyber law: Safeguarding digital spaces in Uzbekistan. *International Journal of Cyber Law, 1*(5). https://doi.org/10.59022/ijcl.53

AllahRakha, N. (2023). Ensuring cyber-security in remote workforce: Legal implications and international best practices. *International Journal of Law and Policy, 1*(3). https://doi.org/10.59022/ijlp.43

Assaf, A. (2023). Violations of sovereignty in "cyberspace" under the United Nations Charter. *HSE University Journal of International Law, 1*(3), 4–20. https://doi.org/10.17323/jil.2023.18848

Balarabe, K. (2025). Digital borders and beyond: Establishing normative grounds for cybersecurity and sovereignty in international law. *Computer Law & Security Review, 58*, 106180. https://doi.org/10.1016/j.clsr.2025.106180

Banks, W. C. (2019). The bumpy road to a meaningful international law of cyber attribution. *AJIL Unbound, 113*, 191–196. https://doi.org/10.1017/aju.2019.32

Banks, W. C. (2021). Cyber attribution and state responsibility. *International Law Studies, 97*, 1039–1072. https://doi.org/10.5038/1944-0472.4.2.3

Beisenbayev, E. (2026). Parliamentary discourse and legislative approaches to cyber sovereignty. *Frontiers in Political Science, 8*, 1874183. https://doi.org/10.3389/fpos.2026.1874183

Boutin, B. (2023). State responsibility in relation to military applications of artificial intelligence. *Leiden Journal of International Law, 36*(1), 133–150. https://doi.org/10.1017/S0922156522000607

Broeders, D. (2024). Cyber intelligence and international security: Breaking the legal and diplomatic silence? *Intelligence and National Security, 39*(6), 1–18. https://doi.org/10.1080/02684527.2024.2398077

Buchan, R. (2016). Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of cyber operations by non-State actors. *Journal of Conflict and Security Law, 21*(3), 405–428. https://doi.org/10.1093/jcsl/krw017

Carpenter, C. (2025). Whose crime is it anyway? State responsibility and individual criminal responsibility in cyberspace. *Journal of International Criminal Justice, 23*(1), 69–85. https://doi.org/10.1093/jicj/mqae005

Corn, G. P., & Taylor, R. (2017). Sovereignty in the age of cyber. *AJIL Unbound, 111*, 207–212. https://doi.org/10.1017/aju.2017.57

Delerue, F. (2020). *Cyber operations and international law*. Cambridge University Press. https://doi.org/10.1017/9781108780605

Di Scipio, J. (2021). Developing an international framework for addressing non-state actors in cyberspace. *Undergraduate Research Journal, 5*(1), 1–15. https://doi.org/10.25776/qzby-ga54

Dinniss, H. H. (2012). *Cyber warfare and the laws of war*. Cambridge University Press. https://doi.org/10.1017/CBO9781139061285

Ducheine, P. A. L., & Pijpers, P. B. M. J. (2021). The notion of cyber operations. In N. Tsagourias & R. Buchan (Eds.), *Research handbook on international law and cyberspace* (2nd ed., pp. 285–306). Edward Elgar Publishing. https://doi.org/10.4337/9781789904253.00024

Egloff, F. J., & Smeets, M. (2023). Publicly attributing cyber attacks: A framework. *Journal of Strategic Studies, 46*(3), 502–533. https://doi.org/10.1080/01402390.2021.1895117

Eichensehr, K. (2017). Cybersecurity & the new systems of collective defense. *Virginia Journal of International Law, 57*, 55–112. https://doi.org/10.2139/ssrn.2907855

Finlay, L., & Payne, C. (2019). The attribution problem and cyber armed attacks. *American Journal of International Law, 113*, 202–206. https://doi.org/10.1017/aju.2019.35

Ghannadi, A. R. (2025). Artificial intelligence and international law: Challenges and opportunities. *Legal Studies in Digital Age, 5*(1), 1–15. https://doi.org/10.61838/kman.lsda.207

Gill, T. D., & Tsagourias, N. (2015). The 2008 cyber operations in the Georgia-Russia conflict. *Yearbook of International Humanitarian Law, 14*, 311–333. https://doi.org/10.1007/978-94-6236-017-4_10

Haataja, S. (2023). Complicity in unlawful offensive cyber operations under international law on state responsibility. *European Conference on Cyber Warfare and Security Proceedings*, 1–10. https://doi.org/10.34190/eccws.22.1.1114

Hakimi, M. (2019). Introduction to the symposium on cyber attribution. *AJIL Unbound, 113*, 189–190. https://doi.org/10.1017/aju.2019.30

Henrico, S. (2025). Cyber attacks in South Africa: Geopolitical and legal implications. *Nnamdi Azikiwe Journal of Political Science, 8*(1), 101–115. https://doi.org/10.1080/10246029.2025.2489352

Hidalgo, E. S., Calleja, A., & Espelt, R. (2024). Co-creation of the Digital Democracy and Data Commons Manifesto: Alternative sociotechnical visions of data. *Open Research Europe, 4*, 45. https://doi.org/10.12688/openreseurope.17020.2

Hulkó, G. (2025). The politics of digital sovereignty and the European Union. *Frontiers in Political Science, 7*, 1548562. https://doi.org/10.3389/fpos.2025.1548562

Kajander, A., Liivoja, R., & Naagel, M. (2025). Cybersecurity of weapon systems: International law requirements and technical standards. *Journal of Cybersecurity, 11*(1), tyaf017. https://doi.org/10.1093/cybsec/tyaf017

Leventopoulos, S. (2024). Retaliating against cyber-attacks: A decision-taking framework for policy makers. *AI & Society, 39*(1), 1–15. https://doi.org/10.1365/s43439-024-00113-5

Liebetrau, T. (2022). Cyber conflict short of war: A European strategic vacuum. *European Security, 31*(4), 497–516. https://doi.org/10.1080/09662839.2022.2031991

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies, 22*(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

Lindsay, J. R. (2015). Tipping the scales: The attribution problem and the feasibility of cyber deterrence. *Journal of Cybersecurity, 1*(1), 53–67. https://doi.org/10.1093/cybsec/tyv003

Mačák, K. (2021). Unblurring the lines: Military cyber operations and international law. *Journal of Cyber Policy, 6*(3), 411–428. https://doi.org/10.1080/23738871.2021.2014919

Marelli, M. (2022). The SolarWinds hack: Lessons for international humanitarian organizations. *International Review of the Red Cross, 104*(919), 1–25. https://doi.org/10.1017/S181638312200025X

Pierucci, F. (2025). Sovereignty in the digital era: Rethinking territoriality and state responsibility in cyberspace. *Digital Society, 4*(1), 1–15. https://doi.org/10.1007/s44206-025-00189-4

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review, 9*(4). https://doi.org/10.14763/2020.4.1532

Popalzay, A. W. (2025). The evolving landscape of the Israel–Iran conflict 2024–2025: Cyber warfare and precision-guided munitions. *Journal of Cybersecurity and International Affairs, 2*(1), 1–15. https://doi.org/10.1142/S2630531325500179

Prasad, N., Diro, A., Warren, M., & Fernando, M. (2025). A survey of cyber threat attribution: Challenges, techniques, and future directions. *Computers & Security, 157*, 104606. https://doi.org/10.1016/j.cose.2025.104606

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1-2), 4–37. https://doi.org/10.1080/01402390.2014.977382

Roberts, H. (2024). Digital sovereignty and artificial intelligence: A normative approach. *Ethics and Information Technology, 26*(4), 70. https://doi.org/10.1007/s10676-024-09810-5

Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press. https://doi.org/10.1017/9781316822524

Spector, P. (2017). In defense of sovereignty, in the wake of Tallinn 2.0. *AJIL Unbound, 111*, 205–206. https://doi.org/10.1017/aju.2017.58

Su, C. (2023). A comparative study on TikTok's data policy: How to think about cyber sovereignty. *Chinese Journal of Communication, 13*(1), 8–26. https://doi.org/10.1080/17544750.2019.1687536

Sukumar, A., & Basu, A. (2024). Back to the territorial state: China and Russia's use of UN cybercrime negotiations to challenge the liberal cyber order. *Journal of Cyber Policy, 9*(2), 256–287. https://doi.org/10.1080/23738871.2024.2436591

Thumfart, J. (2020). Public and private just wars: Distributed cyber deterrence based on Vitoria and Grotius. *Internet Policy Review, 9*(3). https://doi.org/10.14763/2020.3.1500

Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law, 17*(2), 229–244. https://doi.org/10.1093/jcsl/krs013

Zhang, C. (2025). A cross-national comparative study of metaverse policy and digital sovereignty. *Politics and Governance, 13*(1), 1–15. https://doi.org/10.17645/pag.10239