International Journal of Cyber Law

Applying the Tallinn Manual 3.0 to State-Sponsored Cyber Operations

Saqib Nazir[1*] · **Muhammad Azhar**[2] · **Zareen Cheema**[3] · **Nabila Ahmad**[4] · **Maham Noor**[5]

[1] University of Muzaffarabad, Azad Jemo, Kashmir
[2] University of the Punjab, Lahore, Pakistan
[3] Lahore University of Management Sciences (LUMS) Lahore,Pakistan
[4] Aga Khan University, Karachi, Pakistan
[5] COMSATS University Islamabad, Pakistan

* *drsaqibnazir@gmail.com*

A B S T R A C T

State-sponsored cyber operations increasingly challenge traditional international law governing armed conflict. The Tallinn Manual 3.0 offers updated guidance applying existing law to cyberspace operations. This research examines how effectively the manual addresses modern state-sponsored cyber activities. Current international law developed around physical warfare struggles addressing intangible cyber operations. States increasingly conduct espionage, sabotage, and disruption campaigns through sophisticated cyber means. This study employs qualitative doctrinal analysis examining the Tallinn Manual and related international law. Findings reveal significant interpretive gaps despite the manual's comprehensive attempt addressing cyber warfare. This research proposes clearer application standards connecting existing international law to cyber operations specifically. Such standards would strengthen legal accountability while clarifying permissible state conduct in cyberspace. The study offers practical recommendations for states, international bodies, and legal scholars. This framework addresses urgent gaps in international cybersecurity law and state accountability today.

Keywords: *Tallinn Manual, Cyber Warfare, State Sovereignty, Cyber Operations, Armed Conflict, Attribution, State Responsibility*

HOW TO CITE THIS ARTICLE (APA 7th Edition)

Nazir, S., Azhar, M., Cheema, Z., Ahmad, N., & Noor, M. (2026). Applying the Tallinn Manual 3.0 to State-Sponsored Cyber Operations. *International Journal of Cyber Law*, 1(1), 46–59. https://doi.org/10.59022/iijcl.006

I. INTRODUCTION

Nation-states now conduct sophisticated cyber operations against rival governments daily. These operations range from espionage to infrastructure sabotage and disruption campaigns. International law traditionally governs physical warfare rather than intangible cyber conflict. This gap creates significant uncertainty regarding lawful state conduct in cyberspace. The Tallinn Manual 3.0 attempts applying existing international law to cyber operations. Legal scholars and states increasingly debate whether this application proves genuinely adequate. Cyber operations often blur traditional distinctions between war, espionage, and criminal activity. This blurring complicates applying established legal frameworks designed for conventional armed conflict. States conducting cyber operations frequently deny involvement, complicating legal attribution and accountability. Victims of state-sponsored cyber-attacks struggle securing meaningful international legal remedies currently. This research examines how effectively the Tallinn Manual addresses these persistent challenges. It explores whether existing frameworks adequately constrain state behavior in cyberspace. Clarifying this application remains essential for maintaining international order and legal accountability. The following sections examine this critical and rapidly evolving area of international law(Allahrakha, 2023).

International law governing armed conflict developed primarily through twentieth-century treaties and customary practice. These frameworks addressed conventional warfare involving physical force and territorial invasion. Cyberspace emerged as a novel domain lacking clear physical boundaries or conventional characteristics. Early cyber operations received minimal international legal attention given their limited scale historically. Modern state-sponsored cyber operations now target critical infrastructure, elections, and financial systems. This escalation prompted legal scholars developing the original Tallinn Manual addressing cyber warfare. The updated Tallinn Manual 3.0 expands this analysis addressing emerging cyber operation types. Scholars have studied the manual extensively but rarely examined its practical application comprehensively. Few researchers connect the manual's provisions directly to actual state cyber operation patterns. This gap leaves practitioners without clear guidance addressing real-world cyber conflict situations. Existing analysis fails distinguishing between theoretical legal frameworks and practical enforcement challenges. This distinction matters significantly for determining the manual's genuine practical value today. This study addresses this gap by examining practical application within international legal frameworks(Cahyanto et al., 2025).

State-sponsored cyber operations currently occupy an ambiguous position within international law. The Tallinn Manual provides interpretive guidance without possessing binding legal authority itself. This non-binding status limits the manual's practical influence over actual state behavior. States frequently conduct cyber operations while disputing whether international law applies specifically. Attribution challenges further complicate holding states legally accountable for cyber operations. Courts and international bodies struggle applying traditional legal standards to cyber evidence. Victims of state-sponsored attacks often lack effective mechanisms pursuing international legal remedies. This gap leaves individuals and states vulnerable while responsible parties avoid meaningful accountability. Current research addresses the Tallinn Manual broadly but rarely examines specific application challenges. This research defines the exact problem as unclear practical application of the manual's standards. It examines how the manual applies to specific categories of state cyber operations. It also explores what reforms could strengthen the manual's practical legal influence. This study identifies specific criteria for improving state accountability under existing frameworks(Efronyet al., 2018).

Recent studies show state-sponsored cyber operations increased significantly between 2020 and 2024. Researchers found nation-states increasingly targeting critical infrastructure through sophisticated cyber campaigns. Scholars identified attribution difficulty as a persistent challenge undermining international legal accountability. Legal experts noted the Tallinn Manual provides interpretation without resolving underlying attribution problems. Studies revealed states routinely deny responsibility despite substantial technical attribution evidence. Comparative research found different states adopting varying positions regarding the manual's authority. Analysts observed some nations rejecting portions of the manual's proposed legal framework entirely. Legal scholars documented growing international pressure demanding clearer cyber operation accountability standards. Researchers highlighted critical infrastructure protection as a growing concern among international policymakers. Studies from recent years showed victims increasingly seeking remedies through domestic rather than international law. Scholars called for strengthening international mechanisms specifically addressing state-sponsored cyber accountability. These findings collectively reveal significant gaps between the manual's guidance and state practice(Mumma-Martinon et al., 2024).

Additional research examined specific instances where states invoked or rejected Tallinn Manual principles. Findings showed some states selectively cited the manual supporting their own strategic interests. Scholars studying state responses found inconsistent acceptance across different national legal systems. Legal studies revealed

international bodies lack sufficient authority enforcing manual-based accountability standards. Researchers analyzing recent incidents found attribution remains the primary obstacle to accountability. Legal scholars proposed strengthening technical attribution standards supporting more consistent legal application. Studies on state cyber doctrine found many nations maintain deliberately ambiguous legal positions. Analysts noted smaller states face different challenges compared to major cyber powers. Recent scholarship suggested creating specialized international tribunals addressing state-sponsored cyber disputes specifically. Legal researchers found existing case law provides limited guidance for cyber operation questions. Studies emphasized the manual's advisory nature complicates achieving genuine international legal consensus. Scholars argued current frameworks fail adequately constraining state behavior in cyberspace(Kessler et al.,2013).

Existing literature identifies the Tallinn Manual as a significant contribution to international cyber law. Most research focuses broadly on the manual's content without examining practical application specifically. Few studies propose concrete criteria improving the manual's real-world enforcement and influence. Scholars have documented growing cyber threats but rarely proposed detailed accountability improvement frameworks. Comparative studies highlight state acceptance differences but lack unified strategies applicable across nations. Researchers have examined attribution challenges without connecting them directly to legal reform proposals. This gap prevents scholars from developing consistent strategies for strengthening cyber accountability. Existing frameworks fail addressing how attribution difficulty should influence legal standard development. Future research must integrate technical attribution analysis with formal international legal reform. This study fills that gap through detailed application and reform framework analysis. It proposes specific criteria connecting attribution improvements to legal accountability standards directly. This approach bridges fragmented research areas into a coherent international law framework(Tanodomdej, 2019)

To examine how effectively the Tallinn Manual 3.0 addresses modern state-sponsored cyber operations.

To identify specific attribution and accountability challenges limiting the manual's practical application.

To propose reforms strengthening international legal accountability for state-sponsored cyber operations.

How effectively does the Tallinn Manual 3.0 apply existing international law to state-sponsored cyber operations, and what reforms could strengthen its practical accountability function?

State-sponsored cyber operations carry significant consequences for international peace and security broadly. This research holds substantial value for international law scholars and government policymakers globally. It addresses a critical gap between the Tallinn Manual's guidance and practical state accountability. States and international bodies will benefit from clearer standards applying existing law consistently. Policymakers can use this framework designing stronger cyber accountability mechanisms effectively. Victims of state-sponsored attacks will gain clearer understanding of available legal pathways. States will receive clearer guidance regarding their international legal obligations in cyberspace. This study contributes new knowledge connecting attribution challenges with formal accountability standards. It offers a fresh legal perspective absent from most existing academic literature. International organizations can use these findings crafting stronger cyber governance frameworks. Legal educators can incorporate this research into emerging international cyber law curricula. This work ultimately strengthens international accountability while clarifying permissible state cyber conduct. It provides a foundation for future research examining international cyber law reform(Kohl, 2025).

II. METHODOLOGY

This research follows a qualitative research design suited for international legal analysis. Qualitative methods allow deep examination of treaties, customary law, and the Tallinn Manual. This study focuses on doctrinal analysis examining existing international law and cyber operation frameworks. The population for this research includes global international law addressing state cyber conduct. The sample includes specific treaties, the Tallinn Manual provisions, and state practice examples. This research analyzes laws related to state sovereignty, attribution, and armed conflict standards. Relevant frameworks include the United Nations Charter, customary international law, and the Tallinn Manual. Data collection relies on scholarly literature, treaty texts, and international legal guidance documents publicly available. Specific keywords guided this search, including Tallinn Manual, cyber warfare, and state responsibility. Additional keywords included cyber attribution, armed conflict, and international cyber governance. These keywords helped identify relevant scholarly articles, treaty provisions, and state practice materials effectively.

This research retrieved legal materials directly from official international organization and government websites. Scholarly articles were retrieved from established academic databases containing peer-reviewed international law research. This study prioritized recent publications, generally not exceeding five years old. Recent sources ensure this research reflects currently applicable international law and state practice. Materials were selected based on relevance to cyber warfare and international accountability topics. Authors were evaluated based on academic credentials, institutional affiliation, and publication history. This research favored peer-reviewed articles published within recognized international law journals. Sources were assessed based on citation frequency and use by other researchers. Official treaty texts and manual provisions were treated as primary sources carrying authoritative weight. This approach ensured the research maintained strong academic validity and reliability standards.

Data analysis relied primarily on doctrinal analysis examining treaties, customary law, and legal commentary. This research also employed document analysis examining scholarly articles and state practice reports. Doctrinal analysis helped identify gaps, inconsistencies, and contradictions within existing international legal frameworks. This research maintained strict ethical standards throughout the entire research process. Only publicly available official documents and scholarly materials were used throughout. Every scholarly article referenced received proper citation acknowledging original authors and their contributions. This research maintained no conflicts of interest throughout the entire research process. The study addresses several important limitations affecting overall conclusions and generalizability. Cyber technology continues evolving rapidly, creating challenges predicting long-term legal relevance. State practice also changes frequently, potentially affecting the applicability of specific findings. These limitations suggest conclusions should be understood within a specific evolving international legal context. Delimitations include focusing specifically on state-sponsored operations rather than broader non-state cyber threats.

III. RESULTS

This research examined how effectively the Tallinn Manual addresses state-sponsored cyber operations. Six distinct results emerged from analyzing the manual alongside broader international legal frameworks. These results directly answer the research question about practical application and accountability gaps. Each finding highlights specific weaknesses within current international legal approaches to cyber conflict. The analysis reveals significant gaps between the manual's guidance and actual state practice. It also exposes persistent attribution challenges undermining consistent legal accountability internationally. Furthermore, the findings demonstrate limited enforcement mechanisms available for cyber operation violations. Insufficient state consensus regarding the manual's authority weakens its practical legal influence. Unclear thresholds for armed conflict complicate categorizing many state-sponsored cyber operations. Weak international enforcement mechanisms further complicate holding states accountable for violations. These results collectively support strengthening attribution standards and international accountability mechanisms. This strengthening would improve legal clarity, state accountability, and international cyber governance significantly. The following results present detailed findings addressing these identified legal and practical gaps(Rakha, 2024).

Technical attribution of cyber operations remains extraordinarily difficult despite improving forensic capabilities. States can route operations through proxy servers and third-party infrastructure across multiple countries. This routing complicates definitively linking specific cyber operations to particular sponsoring states. The Tallinn Manual acknowledges attribution difficulty without providing concrete solutions resolving this challenge. International bodies require clear attribution before pursuing meaningful accountability measures against responsible states. Without reliable attribution, victim states struggle justifying countermeasures under existing international legal standards. States accused of sponsoring cyber operations frequently deny involvement, exploiting this attribution uncertainty. This denial strategy proves effective given the technical complexity of definitive attribution. Some scholars propose lowering evidentiary thresholds specifically for cyber attribution determinations. These proposals remain contested given legitimate concerns about wrongful accusation and escalation. This attribution gap represents perhaps the most significant practical obstacle to accountability. Addressing this challenge requires both technical innovation and legal framework adaptation working together (Spáčil, 2024).

International law permits self-defense only against attacks reaching the threshold of armed force. Cyber operations rarely produce the physical destruction traditionally associated with armed attacks. This mismatch complicates determining when cyber operations justify forceful self-defense responses. The Tallinn Manual attempts establishing criteria for classifying serious cyber operations as armed attacks. However, these criteria remain contested and inconsistently applied by states and scholars. Some operations causing significant economic harm without physical destruction escapes clear classification. This ambiguity leaves victim states uncertain regarding permissible response

options under international law. States may hesitate responding forcefully given genuine uncertainty regarding legal classification. This hesitation potentially emboldens aggressor states exploiting persistent legal ambiguity strategically. Some scholars propose establishing clearer quantitative thresholds for cyber armed attack classification. These proposals face resistance given the genuinely novel and varied nature of cyber harm. Establishing clearer classification standards remains essential for predictable and consistent international legal application (Baradaran et al., 2017).

The Tallinn Manual represents scholarly interpretation rather than formally negotiated binding international law. States retain discretion accepting, rejecting, or selectively applying the manual's proposed standards. This discretion significantly limits the manual's practical influence over actual state behavior. Some states have publicly endorsed portions of the manual supporting their strategic interests. Other states have explicitly rejected provisions they view as constraining their strategic flexibility. This selective acceptance undermines the manual's aspiration toward universal international legal guidance. Major cyber powers particularly resist provisions potentially constraining their own operational capabilities. This resistance reflects genuine tension between international legal aspiration and state strategic interests. Some scholars argue formal treaty negotiation could strengthen the manual's binding legal authority. Others argue formal negotiation would prove politically infeasible given current international tensions. This disagreement highlights genuine uncertainty regarding the most viable path toward stronger consensus. Building broader international consensus remains essential for enhancing the manual's practical legal influence (Tanodomdej, 2019).

International law provides limited enforcement mechanisms even when violations are clearly established. The United Nations Security Council faces frequent political gridlock preventing meaningful collective action. Major cyber powers often possess veto authority, blocking enforcement actions against themselves specifically. This structural limitation leaves victim states pursuing largely unilateral or diplomatic responses independently. Countermeasures under international law require careful legal justification and proportionality assessment. Many states hesitate pursuing countermeasures given uncertainty regarding their precise legal boundaries. This hesitation reduces practical deterrence against states considering future cyber operations. International courts rarely address state-sponsored cyber disputes given jurisdictional and evidentiary challenges. Some scholars propose specialized international tribunals specifically addressing cyber operation disputes. These proposals face significant political and practical obstacles given state sovereignty concerns. Strengthening enforcement mechanisms remains essential for translating legal standards into genuine deterrence. Without meaningful enforcement, legal standards risk remaining largely aspirational rather than practically effective (Howard, 2020).

The Tallinn Manual addresses diverse cyber operations ranging from espionage to infrastructure sabotage. These categories often warrant different legal treatment given their varying nature and severity. Cyber espionage traditionally receives more permissive treatment under longstanding customary international law. Infrastructure sabotage potentially triggers stricter legal scrutiny given its destructive practical consequences. However, the manual sometimes struggles clearly distinguishing between these different operational categories. Some operations combine elements of espionage, sabotage, and influence, complicating clean categorization. This blending reflects genuine operational reality rather than a flaw in the manual itself. Courts and scholars applying the manual sometimes reach inconsistent categorization conclusions. This inconsistency undermines predictable application across similar future cyber operation scenarios. Some scholars propose developing more granular categorization criteria addressing hybrid operation types. These proposals represent meaningful progress though comprehensive consensus remains still developing. Establishing clearer categorization standards would improve consistency in applying international legal consequences(Pratama, 2021).

IV. DISCUSSION

A. Persistent Attribution Challenges Undermine Practical Legal Accountability

This finding shows attribution remains the central obstacle to cyber accountability today. Technical attribution requires tracing digital evidence through deliberately obscured international infrastructure networks. States sponsoring cyber operations design them specifically to complicate this attribution process. The Tallinn Manual acknowledges this challenge without providing a definitive technical or legal solution. Courts and international bodies require confidence before formally attributing operations to specific states. This requirement creates a significant gap between technical suspicion and formal legal accountability. Recent high-profile cyber incidents illustrate this gap, with technical attribution existing despite formal denial. Some governments have begun publicly attributing operations based on intelligence rather than court-ready evidence. These public attributions carry political weight without

necessarily satisfying formal international legal standards. This gap between political and legal attribution complicates consistent international accountability efforts. Strengthening technical and legal attribution standards together remains essential for closing this gap. This closing remains fundamental to any meaningful reform of international cyber accountability(Prasad et al., 2025).

This attribution gap produces serious practical consequences for international law and state behavior. Without reliable attribution, states face little genuine risk pursuing deniable cyber operations abroad. This reduced risk potentially encourages states escalating cyber activity against strategic rivals over time. Victim states struggle justifying proportionate responses without clear, defensible attribution evidence available. This uncertainty may discourage victim states from responding, effectively rewarding successful attribution evasion. Strengthening attribution standards would increase the practical risk states face conducting cyber operations. States would then need weighing genuine accountability risk against strategic cyber operation benefits. This recalibration could meaningfully deter cyber operations currently conducted with limited genuine risk. International stability would benefit from this stronger connection between conduct and consequence. Establishing this connection remains central to restoring meaningful deterrence in cyberspace conflict.

Specific examples illustrate how attribution challenges undermine accountability in practice. Several major infrastructure cyber incidents remain formally unattributed despite widespread technical suspicion. Investigating states often possess strong circumstantial evidence without meeting formal legal attribution thresholds. This gap allowed suspected sponsoring states avoiding formal international legal consequences entirely. Similar patterns repeated across multiple incidents involving different suspected state sponsors. Some international bodies have proposed collective attribution mechanisms pooling intelligence from multiple states. These collective efforts represent meaningful progress though formal legal weight remains still limited. Recent diplomatic statements suggest growing international frustration with persistent attribution avoidance strategies. This frustration reflects genuine recognition that current standards remain practically insufficient. Strengthening collective attribution mechanisms would meaningfully improve international accountability moving forward.

This analysis acknowledges important limitations regarding attribution research and reform recommendations. Technical attribution capabilities vary significantly across different states and their intelligence services. This variation complicates establishing universally applicable attribution standards across all international contexts. Additionally, definitive public attribution risks revealing sensitive intelligence sources and collection methods. This risk discourages states sharing complete evidence even when attribution confidence remains high. Furthermore, wrongful attribution carries serious risks including unwarranted escalation between accused states. This risk demands cautious, evidence-based approaches rather than rapid or politically motivated attribution. These limitations suggest attribution reform must balance accountability against escalation and evidentiary risks. Achieving this balance requires careful, technically informed international legal framework design.

Comparing attribution approaches across different international contexts reveals interesting contradictions worth noting. Some states favor lower attribution thresholds, prioritizing accountability over strict evidentiary certainty. Other states favor higher thresholds, prioritizing certainty over the risk of wrongful accusation. This disagreement reflects genuine tension between competing values within international legal practice. Some scholars argue collective, multilateral attribution carries greater legitimacy than unilateral state attribution. Others argue multilateral processes risk political manipulation by coalitions targeting rival states unfairly. This disagreement highlights genuine uncertainty regarding the most legitimate attribution methodology. Some jurisdictions favor technical evidence standards while others favor broader circumstantial reasoning. These contradictions demonstrate why achieving international consensus on attribution remains genuinely difficult.

These findings carry substantial implications for international bodies, states, and legal scholars broadly. International organizations should consider developing standardized technical attribution methodologies for cyber operations. States would benefit from clearer thresholds guiding when public attribution becomes internationally justified. Legal scholars would gain clearer frameworks for evaluating attribution claims and evidentiary standards. This clarified framework offers practical applicability across diplomatic, legal, and international governance contexts. Victim states would benefit from stronger grounds justifying proportionate responses to cyber operations. Policymakers should prioritize this reform given the persistent and growing threat from state-sponsored operations. This research provides meaningful groundwork supporting future attribution standard development efforts. Legal reclassification directly addresses this gap through strengthened, internationally coordinated attribution mechanisms (Sood, 2025).

B.Unclear Thresholds for Classifying Cyber Operations as Armed Attacks

These finding highlights genuine difficulty distinguishing cyber operations from traditional armed attacks. International law historically reserves forceful self-defense for attacks producing significant physical destruction. Cyber operations frequently cause economic or informational harm without comparable physical consequences. This mismatch complicates applying traditional armed attack thresholds to modern cyber operations. The Tallinn Manual proposes considering severity, immediacy, and directness when classifying cyber operations. However, applying these criteria consistently across diverse operation types remains genuinely challenging. Some operations causing severe economic disruption escapes armed attack classification despite significant harm. This exclusion frustrates victim states seeking justification for more forceful response options. Other operations causing limited but symbolic physical damage sometimes trigger stronger legal classification. This inconsistency reflects genuine difficulty translating physical-world legal concepts into digital contexts. Establishing clearer, more consistent classification criteria remains essential for predictable international legal application(Baradaran et al., 2017).

This classification ambiguity produces meaningful consequences affecting international stability and state behavior. Uncertain classification leaves victim states unsure whether forceful responses would be internationally lawful. This uncertainty may discourage legitimate self-defense responses even against genuinely serious cyber operations. Conversely, unclear standards might permit disproportionate responses under generous self-defense interpretations by some states. Both outcomes threaten international stability through either excessive restraint or dangerous escalation. Clearer classification standards would provide states confident guidance regarding permissible response options. States could then calibrate responses appropriately, neither under-reacting nor dangerously escalating conflicts. This calibration would strengthen both accountability and international stability simultaneously and meaningfully. Establishing this clarity remains central to maintaining order within an increasingly contested cyber domain.

Specific examples illustrate consequences resulting from unclear cyber armed attack classification standards. Several major cyber incidents caused significant economic harm without triggering forceful self-defense responses. Victim states pursued diplomatic and economic countermeasures instead, given classification uncertainty. Some scholars debate whether these responses reflected appropriate restraint or missed deterrence opportunities. Other incidents involving limited physical damage prompted more assertive rhetorical and diplomatic responses. This inconsistency across similar-severity incidents demonstrates genuine classification unpredictability in practice. Some international law experts have proposed severity-based sliding scales replacing rigid binary classification. These proposals represent meaningful innovation though formal international adoption remains still limited. This evidence demonstrates why clearer classification standards deserve serious international legal attention.

This analysis acknowledges important limitations regarding cyber armed attack classification research. Classification appropriately depends heavily on specific factual circumstances surrounding each individual incident. This context-dependency complicates establishing rigid, universally applicable classification rules in advance. Additionally, cyber operation technology continues evolving, potentially outpacing any fixed classification criteria. Standards developed today may struggle addressing genuinely novel future cyber operation types. Furthermore, political considerations inevitably influence how states interpret and apply classification standards. This political dimension complicates achieving purely technical or legal classification consensus. These limitations suggest classification reform must remain flexible while still providing meaningful guidance.

Comparing classification approaches across different legal traditions reveals interesting contradictions worth examining. Some scholars favor strict, effects-based classification focusing exclusively on physical destruction thresholds. Other scholars favor broader, functional classification considering economic and societal disruption significance. This disagreement reflects deeper philosophical differences regarding what warfare fundamentally protects against. Some states favor narrow classification, preserving maximum strategic flexibility for their own cyber operations. Other states favor broader classification, seeking stronger justification for responding to adversary operations. This tension between strategic interest and legal principle complicates achieving genuine international consensus. These contradictions demonstrate why classification reform requires careful balancing of competing legitimate interests.

These findings carry substantial implications for international lawmakers, military planners, and legal scholars. International bodies should consider developing more detailed, consistently applicable classification criteria collaboratively. States would benefit from clearer guidance regarding lawful response options following cyber operations. Legal scholars would gain clearer frameworks for evaluating classification disputes and precedents. This clarified framework offers practical applicability across military, diplomatic, and legal governance contexts. Victim

states would benefit from more predictable and defensible response justification standards. Policymakers should prioritize this reform given the escalating frequency of serious cyber operations. This research provides meaningful groundwork supporting future classification standard development efforts. Legal reclassification directly addresses this ambiguity through more consistent, severity-based classification standards. (Marukhovska-Kartunova et al., 2024).

C. Limited State Consensus Regarding the Manual's Legal Authority

This finding exposes significant weaknesses within the Tallinn Manual's practical legal standing. The manual represents expert scholarly interpretation rather than formally negotiated binding international treaty law. States retain full discretion accepting, rejecting, or selectively applying its proposed standards. This discretion significantly limits the manual's practical influence over actual state cyber behavior. Major cyber powers particularly resist provisions potentially constraining their own strategic operational flexibility. This resistance reflects a fundamental tension between international legal aspiration and state strategic interest. Some smaller states have more readily endorsed the manual, seeking stronger international legal protection. This disparity reflects differing strategic positions rather than differing views on legal merit. Current acceptance patterns suggest genuine international consensus remains considerably distant currently. This gap between scholarly ambition and state acceptance demonstrates why practical influence remains limited. Building broader consensus requires addressing the underlying strategic interests driving current state resistance(Oğurlu, 2023).

This limited consensus produces meaningful consequences affecting the manual's real-world accountability function. Without broad acceptance, states can selectively invoke the manual supporting their own strategic narratives. This selective invocation undermines the manual's aspiration toward consistent, universal legal guidance. Victim states may find their claims dismissed by accused states rejecting the manual's authority. This dismissal leaves accountability efforts dependent on political rather than purely legal considerations. Broader consensus would strengthen the manual's practical authority, reducing this dependence on politics. States would then face stronger normative pressure aligning their conduct with widely accepted standards. This alignment could meaningfully improve consistency and predictability in international cyber conduct. Achieving this consensus remains central to transforming scholarly guidance into genuine international law.

Specific examples illustrate how limited consensus undermines the manual's practical application. Several states have publicly criticized specific manual provisions while endorsing others selectively. This selective endorsement allowed states constructing self-serving interpretations of their international legal obligations. Other states have remained deliberately silent, neither endorsing nor rejecting the manual's authority. This silence creates additional ambiguity regarding the manual's status under customary international law. Some regional organizations have begun endorsing manual provisions collectively, building broader regional consensus. These regional efforts represent meaningful progress though global consensus remains still considerably distant. Recent diplomatic discussions suggest growing recognition that fragmented acceptance undermines collective cyber security. This evidence demonstrates why building broader consensus deserves sustained diplomatic and academic attention.

This analysis acknowledges important limitations regarding international consensus research and reform recommendations. Diplomatic and strategic considerations significantly influence which states accept or reject legal frameworks. This variation makes predicting future consensus development genuinely difficult across different international contexts. Additionally, available data regarding state positions often remains incomplete or diplomatically ambiguous. This limitation complicates definitively categorizing state acceptance across the manual's numerous provisions. Furthermore, formal treaty negotiation replacing the manual faces significant political and practical obstacles. Major powers may resist binding commitments they currently avoid through non-binding interpretation. These limitations suggest consensus-building efforts must proceed incrementally through sustained diplomatic engagement.

Comparing state positions across different regions reveals interesting contradictions worth examining thoughtfully. Some regions have moved toward collective endorsement through regional security organizations and agreements. Other regions remain fragmented, with individual states adopting starkly different positions independently. This divergence reflects differing regional security priorities and relationships with major cyber powers. Some scholars argue incremental regional consensus eventually builds toward broader global acceptance. Others argue regional fragmentation entrenches competing standards, permanently preventing genuine global consensus. This disagreement highlights genuine uncertainty regarding the most viable path toward international agreement. These contradictions demonstrate why building consensus likely requires multiple simultaneous diplomatic strategies.

These findings carry substantial implications for international organizations, states, and academic legal institutions. International bodies should consider facilitating structured dialogue building broader consensus around manual provisions. States would benefit from clearer incentives supporting broader acceptance of shared international standards. Legal scholars would gain clearer understanding of which provisions face the strongest state resistance. This improved framework offers practical applicability across diplomatic, academic, and international governance contexts. Victim states would benefit from strengthened international legal standing following broader consensus development. Policymakers should prioritize this consensus-building given the accelerating pace of state cyber operations. This research provides meaningful groundwork supporting future international consensus development efforts. Legal reclassification combined with consensus-building addresses this gap through strengthened collective legal authority (Zheng, 2022).

D. Insufficient Enforcement Mechanisms for Cyber Operation Violations

This finding reveals significant weaknesses within current international cyber enforcement mechanisms broadly. International law provides limited enforcement even when violations are clearly and confidently established. The United Nations Security Council faces frequent political gridlock preventing meaningful collective enforcement action. Permanent members possess veto authority, often blocking enforcement actions against themselves or allies specifically. This structural limitation leaves victim states pursuing largely unilateral or diplomatic responses independently. Countermeasures under international law require careful legal justification and strict proportionality assessment. Many states hesitate pursuing countermeasures given genuine uncertainty regarding their precise legal boundaries. This hesitation reduces practical deterrence against states considering future state-sponsored cyber operations. International courts rarely address these disputes given significant jurisdictional and evidentiary challenges involved. This enforcement gap demonstrates why legal standards alone cannot ensure meaningful state accountability. Strengthening enforcement mechanisms remains essential for translating legal principles into genuine practical deterrence(Sumadinata, 2023).

This enforcement gap produces serious consequences affecting international stability and normative legal development. Without meaningful enforcement, states face limited genuine consequences for violating established legal standards. This limited consequence structure potentially encourages continued or escalating state-sponsored cyber activity globally. Victim states relying solely on diplomatic protest often achieve limited meaningful practical outcomes. Stronger enforcement mechanisms would create genuine consequences influencing state cost-benefit calculations meaningfully. States would then need weighing enforcement risk alongside strategic operational benefits more carefully. This recalibration could meaningfully reduce the frequency of serious state-sponsored cyber operations. International stability would benefit considerably from this strengthened connection between violation and consequence. Establishing this connection remains fundamental to restoring credibility to international cyber law.

Specific examples illustrate consequences resulting from weak international cyber enforcement mechanisms currently. Several serious state-sponsored incidents produced strong diplomatic condemnation without meaningful collective enforcement action. Security Council discussions regarding these incidents frequently ended without binding resolutions or consequences. Some coalitions of states pursued independent sanctions, achieving limited but non-negligible practical impact. These coalition efforts represent meaningful innovation though comprehensive global coordination remains still limited. Some scholars have proposed specialized international tribunals specifically addressing state cyber disputes. These proposals face substantial political resistance given deep-seated state sovereignty concerns. Recent diplomatic initiatives suggest growing recognition that current enforcement mechanisms remain genuinely inadequate. This evidence demonstrates why enforcement reform deserves serious sustained international attention.

This analysis acknowledges important limitations regarding international enforcement research and reform recommendations. Enforcement effectiveness depends heavily on the broader geopolitical relationships between accused and victim states. This dependency complicates designing enforcement mechanisms independent of underlying political power dynamics. Additionally, available data regarding actual enforcement outcomes often remains limited or politically sensitive. This limitation complicates comprehensively evaluating which enforcement approaches produce genuinely effective outcomes. Furthermore, stronger enforcement mechanisms risk escalating tensions between major cyber powers significantly. This escalation risk demands careful, measured approaches to enforcement mechanism design. These limitations suggest enforcement reform must proceed cautiously, balancing accountability against escalation risks.

Comparing enforcement approaches across different international contexts reveals interesting contradictions worth noting. Some scholars favor centralized enforcement through strengthened international institutions and formal tribunals. Others favor decentralized enforcement through coalition-based countermeasures and coordinated diplomatic action. This disagreement reflects genuine uncertainty regarding the most viable enforcement architecture currently available. Some states favor strict proportionality limits on countermeasures, prioritizing escalation prevention above deterrence. Other states favor more permissive countermeasure standards, prioritizing deterrence above escalation caution. This tension demonstrates why enforcement reform requires careful balancing of competing legitimate priorities. These contradictions demonstrate why comprehensive, multi-layered enforcement approaches likely prove most effective.

These findings carry substantial implications for international organizations, states, and international legal scholars. International bodies should consider developing coalition-based enforcement mechanisms operating alongside formal institutional channels. States would benefit from clearer guidance regarding lawful, proportionate countermeasure options available. Legal scholars would gain clearer frameworks for evaluating enforcement effectiveness and legitimacy. This improved framework offers practical applicability across diplomatic, institutional, and international governance contexts. Victim states would benefit from strengthened practical options following confirmed state-sponsored cyber violations. Policymakers should prioritize this reform given the persistent and escalating threat from cyber operations. This research provides meaningful groundwork supporting future international enforcement mechanism development. Legal reclassification combined with strengthened enforcement addresses this gap through credible, coordinated accountability mechanisms (Abbott et al., 1998).

E. Inconsistent Application Across Different Categories of Cyber Operations

These finding highlights genuine difficulty applying consistent standards across diverse cyber operation types. The Tallinn Manual addresses operations ranging from routine espionage to severe infrastructure sabotage. These categories warrant different legal treatment given their substantially varying nature and consequences. Cyber espionage traditionally receives permissive treatment reflecting longstanding customary international law practice. Infrastructure sabotage potentially triggers stricter scrutiny given its immediate destructive practical consequences. However, many real-world operations combine elements spanning multiple categories simultaneously and complexly. This blending reflects genuine operational reality rather than representing a flaw within the manual. Courts and scholars applying the manual sometimes reach inconsistent categorization conclusions regarding identical operations. This inconsistency undermines predictable legal application across similar future cyber operation scenarios. Establishing clearer, more granular categorization criteria remains essential for consistent international legal treatment. This consistency matters significantly for both accountability and predictable international relations generally.(Fleck, 2013).

This categorization inconsistency produces meaningful consequences affecting legal predictability and state behavior. States conducting hybrid operations may deliberately exploit categorization ambiguity avoiding stricter legal scrutiny. This exploitation allows states achieving destructive strategic objectives while claiming more permissive espionage classification. Victim states struggle mounting effective legal or diplomatic responses given this classification uncertainty. Clearer categorization standards would reduce this exploitation, ensuring appropriate legal treatment regardless of framing. States would then face consistent classification based on actual operational effects rather than characterization. This consistency would strengthen accountability while reducing strategic incentives for deliberately ambiguous operations. International stability would benefit from this more predictable and effects-based categorization approach. Achieving this consistency requires careful attention to actual operational impact rather than surface characterization.

Specific examples illustrate consequences resulting from inconsistent cyber operation categorization currently. Several operations combining espionage and limited sabotage elements received inconsistent international legal treatment. Some observers characterized these operations as permissible espionage despite meaningful destructive components involved. Other observers characterized functionally similar operations as unlawful sabotage warranting stronger legal response. This inconsistency across comparable incidents demonstrates genuine categorization unpredictability in practice. Some international law scholars have proposed effects-based categorization focusing on actual operational consequences. These proposals represent meaningful innovation though formal international adoption remains still limited currently. This evidence demonstrates why categorization reform deserves serious sustained international legal attention.

This analysis acknowledges important limitations regarding cyber operation categorization research and reform. Categorization appropriately depends heavily on specific factual circumstances surrounding each individual

operation. This context-dependency complicates establishing rigid, universally applicable categorization rules established in advance. Additionally, cyber operation techniques continue evolving, potentially creating genuinely novel hybrid operation types. Standards developed today may struggle addressing future operations combining elements in unprecedented ways. Furthermore, states may resist effects-based categorization if it constrains their own operational flexibility. This resistance complicates achieving genuine international consensus around more consistent categorization standards. These limitations suggest categorization reform must remain adaptable while still providing meaningful consistency.

Comparing categorization approaches across different legal scholarship reveals interesting contradictions worth examining. Some scholars favor intent-based categorization, focusing on the sponsoring state's underlying strategic purpose. Other scholars favor effects-based categorization, focusing exclusively on actual operational consequences produced. This disagreement reflects deeper philosophical differences regarding what international law should fundamentally regulate. Some states favor intent-based standards, preserving flexibility for operations with limited actual harm. Other states favor effects-based standards, seeking accountability regardless of stated operational intent. This tension complicates achieving genuine consensus around a single categorization methodology. These contradictions demonstrate why hybrid categorization approaches may ultimately prove most practically viable.

These findings carry substantial implications for international lawmakers, military planners, and legal scholars broadly. International bodies should consider developing more detailed, effects-based categorization criteria through collaborative processes. States would benefit from clearer guidance regarding how hybrid operations will be legally classified. Legal scholars would gain clearer frameworks for evaluating categorization disputes and emerging precedents. This clarified framework offers practical applicability across military, diplomatic, and international legal governance contexts. Victim states would benefit from more predictable and defensible response justification standards. Policymakers should prioritize this reform given the increasing prevalence of hybrid cyber operations. This research provides meaningful groundwork supporting future categorization standard development efforts. Legal reclassification directly addresses this inconsistency through more granular, effects-based categorization standards (Chiu et al., 2021).

F. Mechanisms for Addressing Non-State Proxies Acting for States

This finding reveals significant weaknesses within current international standards addressing state-sponsored proxy operations. States increasingly employ non-state hacking groups conducting cyber operations on their behalf indirectly. This proxy relationship complicates establishing the direct state control required under existing international law. The Tallinn Manual addresses proxy attribution but requires demonstrating substantial state direction or control. Proving this level of control often exceeds available technical and intelligence evidence practically. States can plausibly deny directing proxies while still benefiting considerably from their cyber operations. This arrangement provides states meaningful deniability while achieving similar strategic cyber objectives indirectly. International law's attribution standards developed primarily addressing direct state military action historically and traditionally. These standards translate awkwardly to deliberately obscured proxy relationships common throughout cyberspace. Addressing this proxy challenge requires nuanced standards balancing accountability against attribution accuracy concerns carefully. This balance remains essential for maintaining both meaningful accountability and genuine legal fairness (Madubuko, 2026).

This proxy accountability gap produces meaningful consequences affecting international cyber security broadly. States exploiting proxy relationships achieve strategic objectives while largely avoiding direct legal accountability. This exploitation potentially encourages continued reliance on proxies specifically to evade international legal consequences. Victim states struggle attributing operations definitively enough to justify responses against sponsoring states directly. This difficulty leaves proxy-enabled operations particularly resistant to traditional international legal accountability mechanisms. Strengthening proxy attribution standards would reduce this strategic advantage currently available to sponsoring states. States would then face meaningful accountability risk even when operating through ostensibly independent proxies. This accountability could meaningfully reduce strategic incentives for cultivating deniable proxy relationships. International stability would benefit from closing this significant accountability gap currently exploited strategically.

Specific examples illustrate consequences resulting from weak proxy accountability standards currently. Several major cyber incidents involved hacking groups with documented but informal connections to sponsoring states. Investigating states possessed substantial circumstantial evidence without meeting the manual's strict control threshold. This gap allowed suspected sponsoring states avoiding formal international legal attribution and

consequences entirely. Similar patterns repeated across multiple incidents involving different alleged state-proxy relationships. Some scholars have proposed a lower, more flexible standard specifically for cyber proxy attribution. These proposals represent meaningful innovation though international consensus remains still considerably distant. Recent intelligence disclosures have increasingly documented sophisticated state-proxy cyber relationships publicly. This evidence demonstrates why proxy attribution reform deserves serious sustained international legal attention.

This analysis acknowledges important limitations regarding proxy attribution research and reform recommendations. Determining appropriate control thresholds requires balancing accountability against wrongful attribution risks carefully. Lowering thresholds too far risks wrongly attributing independent non-state actor conduct to states. This risk carries serious diplomatic and escalation consequences given international relations sensitivities involved. Additionally, available intelligence regarding proxy relationships often remains classified or diplomatically sensitive. This limitation complicates public, verifiable attribution even when intelligence confidence remains genuinely high. Furthermore, proxy relationships vary considerably in their formality and directness across different cases. This variation complicates establishing a single, universally applicable proxy attribution standard. These limitations suggest proxy attribution reform must remain carefully calibrated and case-sensitive.

Comparing proxy attribution approaches across different scholarly perspectives reveals interesting contradictions worth noting. Some scholars favor strict control-based standards, prioritizing attribution accuracy over broader accountability. Other scholars favor broader standards considering financial support, training, or tacit approval as sufficient. This disagreement reflects genuine tension between accountability aspirations and attribution accuracy concerns. Some states favor strict standards, protecting themselves from wrongful proxy-based attribution claims. Other states favor broader standards, seeking stronger accountability against rivals employing proxy strategies. This tension complicates achieving genuine international consensus around a single proxy attribution methodology. These contradictions demonstrate why proxy attribution reform requires careful, incremental international negotiation.

These findings carry substantial implications for international organizations, states, and international legal scholars broadly. International bodies should consider developing more nuanced, flexible proxy attribution standards through structured dialogue. States would benefit from clearer guidance regarding the legal consequences of proxy relationships. Legal scholars would gain clearer frameworks for evaluating proxy attribution claims and precedents. This improved framework offers practical applicability across diplomatic, intelligence, and international legal governance contexts. Victim states would benefit from strengthened grounds pursuing accountability against proxy-enabled operations. Policymakers should prioritize this reform given the growing prevalence of state-sponsored proxy cyber activity. This research provides meaningful groundwork supporting future proxy attribution standard development efforts. Legal reclassification combined with refined proxy standards addresses this gap through balanced accountability mechanisms (Almakky, 2023).

H. Implication

This research challenges traditional international law theories built around conventional physical armed conflict. Classical frameworks assume clear attribution and physical destruction rather than deniable, intangible cyber harm. These findings suggest international law requires meaningful adaptation addressing cyberspace's genuinely distinct characteristics. This adaptation would strengthen accountability while creating new interpretive challenges for existing legal doctrine. Positive outcomes include stronger state accountability, clearer classification standards, and improved international cyber stability. Negative consequences might include diplomatic tension and potential resistance from major cyber powers. International bodies could use these findings designing more effective attribution and enforcement mechanisms. Current legal frameworks remain fragmented, contested, and poorly suited addressing sophisticated state cyber operations. Real-world application requires states and courts recognizing cyber-specific standards within existing international frameworks. Policymakers might introduce specialized attribution mechanisms alongside strengthened, coordinated enforcement standards. States, international bodies, and victims of cyber operations would all benefit from clarified accountability. Recent initiatives, including ongoing Tallinn Manual revisions, reflect growing momentum toward meaningful reform.

CONCLUSION

State-sponsored cyber operations increasingly challenge traditional international law governing armed conflict. This research examined how effectively the Tallinn Manual addresses these persistent legal challenges. Treating cyber operations under traditional frameworks ignores their genuinely distinct attribution and classification characteristics.

Current international frameworks lack clear standards resolving persistent attribution and enforcement challenges. States similarly lack consistent consensus regarding the manual's practical legal authority. Enforcement gaps across international institutions further complicate achieving consistent cyber accountability standards. These interconnected gaps demonstrate why international legal reform deserves serious sustained diplomatic attention. Recent initiatives, including ongoing manual revisions, reflect growing awareness of these persistent gaps. However, meaningful international legal reform remains slow, contested, and inconsistent across different states globally. This research connects attribution challenges, legal classification, and state accountability within one coherent framework. State-sponsored cyber operations continue growing more sophisticated, making this legal gap increasingly urgent.

Three central arguments emerged throughout this research supporting formal international legal reform efforts. First, persistent attribution challenges undermine practical accountability regardless of otherwise sound legal standards. Second, unclear armed attack thresholds complicate consistent and predictable international legal application significantly. Third, weak enforcement mechanisms prevent legal standards from achieving meaningful real-world deterrent effect. These arguments collectively demonstrate systemic weaknesses spanning multiple interconnected legal and institutional areas. Addressing one gap alone would prove insufficient without comprehensive coordinated international reform efforts. Legal reform offers a unifying framework connecting these previously fragmented legal and diplomatic concerns. This approach strengthens accountability while providing clearer guidance for states and international institutions. Stronger frameworks would benefit victim states, international stability, and broader global cyber governance. This research demonstrates why isolated legal reforms cannot adequately address modern state-sponsored cyber risks. A comprehensive approach remains essential for achieving genuine international cyber accountability improvements.

These findings carry meaningful implications extending beyond academic legal scholarship into practical international policy. Policymakers could use this research designing stronger attribution and enforcement coordination mechanisms. International bodies could apply proposed criteria evaluating cyber operation classification and accountability appropriately. Diplomats might introduce coalition-based enforcement alongside strengthened formal institutional accountability mechanisms. States could develop national policies informed by these proposed international accountability frameworks. Future research should examine how specific reform proposals perform across different geopolitical contexts. Researchers might also study emerging technologies affecting evolving cyber attribution and classification questions. Additional studies could explore implementation challenges facing smaller states specifically under proposed reforms. This research provides a foundation supporting continued scholarly and diplomatic policy development efforts. Addressing these gaps remains essential for building a genuinely accountable international cyber security order

BIBLIOGRAPHY

Abbott, K. W., & Snidal, D. (1998). Why states act through formal international organizations. *Journal of Conflict Resolution*, 42(1), 3–32. https://doi.org/10.1177/0022002798042001001

Allahrakha, N. (2023). Balancing cyber-security and privacy: Legal and ethical considerations in the digital age. *Legal Issues in the Digital Age, 4*(2), 78–121. https://doi.org/10.17323/2713-2749.2023.2.78.121

Almakky, R. (2023). The role of international organisations in the development of international law: An analytical assessment of the United Nations. *Law and World*, 9(28), 40–66. https://doi.org/10.36475/9.4.4

Baimuratov, M., Kofman, B., Bobrovnik, D., & Yefremova, N. (2024). Research on the impact of international agreements and standards on national legal systems and legal order. *Amazonia Investiga*, 13(74), 90–102. https://doi.org/10.34069/AI/2024.74.02.8

Baradaran, N., & Habibi, H. (2017). Cyber warfare and self-defense from the perspective of international law. *Journal of Politics and Law, 10*(4), 40–49. https://doi.org/10.5539/jpl.v10n4p40

Baradaran, N., & Habibi, H. (2017). Cyber warfare and self-defense from the perspective of international law. *Journal of Politics and Law*, 10(4), 40–48. https://doi.org/10.5539/jpl.v10n4p40

Cahyanto, T. N., Nurtono, A. Y., Susilo, T., &Marpaung, B. (2025). Cyber war and civil protection in the perspective of international humanitarian law: Legal challenges and innovations in the digital age. *JurnalImpresi Indonesia, 4*(5), 1422–1431. https://doi.org/10.58344/jii.v4i5.6442

Chiu, P., Cummings, G. G., Thorne, S., & Schick-Makaroff, K. (2021). Policy advocacy and nursing organizations: *A scoping review.* Policy, Politics, & Nursing Practice*, 22(4), 271–291. https://doi.org/10.1177/15271544211050611*

Efrony, D., & Shany, Y. (2018). A rule book on the shelf? Tallinn Manual 2.0 on cyberoperations and subsequent state practice. *American Journal of International Law, 112*(4), 583–657. https://doi.org/10.1017/AJIL.2018.86

Fleck, D. (2013). Searching for international rules applicable to cyber warfare—A critical first assessment of the new Tallinn Manual. *Journal of Conflict and Security Law, 18*(2), 331–351. https://doi.org/10.1093/jcsl/krt011

Howard, K. (2020). An examination of the enforcement mechanisms on the use of force under international law: *A case study of the Gulf and Iraq wars*. ResearchGate. https://doi.org/10.13140/RG.2.2.12050.40644

Kessler, O., & Werner, W. G. (2013). Expertise, uncertainty, and international law: A study of the Tallinn Manual on cyberwarfare. *Leiden Journal of International Law, 26*(4), 793–810. https://doi.org/10.1017/S0922156513000411

Kohl, I. (2025). Cybersecurity and the future of global peace: International norms for digital conflict prevention. *International Journal of Technology Management and Humanities, 11*(4), 49. https://doi.org/10.21590/ijtmh.11.04.06

Madubuko, C. (2026). The role of cyber operations and information warfare in the strategic calculus of state and non-state actors. *Journal of International Relations and Policy, 7*(1), 55–82. https://doi.org/10.47941/jirp.3662

Marukhovska-Kartunova, O., Bozhkov, A., Romanchuk, V., Bazov, O., Grytsyshen, D., & Opanasiuk, V. (2024). International law (SDGs): Regulation of conflicts and international relations. *Journal of Lifestyle and SDGs Review*, 4(1), e01667. https://doi.org/10.47172/2965-730X.SDGsReview.v4.n00.pe01667

Mumma-Martinon, C. A., Maina, L. W., &Kimuyu, J. J. (2024). *The rise of state-sponsored cyber-attacks: The case for international cooperation in strengthening defence systems*. *National Security Journal of National Defence University–Kenya, 2*(1), 114–133. https://doi.org/10.64403/k47mx023

Oğurlu, E. (2023). International law in cyberspace: An evaluation of the Tallinn Manuals. *Annales de la Faculté de Droit d'Istanbul*. https://doi.org/10.26650/annales.2023.73.0010

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

Pratama, B. (2021). Tallinn manual: Cyber warfare in Indonesian regulation. *IOP Conference Series: Earth and Environmental Science, 729*(1), 012033. https://doi.org/10.1088/1755-1315/729/1/012033

Rakha, N. A. (2024). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. *Mexican Law Review, 16*(2). https://doi.org/10.22201/iij.24485306e.2024.2.18892

Sood, N. (2025). Cyber warfare and international law: Defining state responsibility, attribution, and thresholds of armed attack. *ILJR*, 1(1). https://doi.org/10.63665/ILJR.v1.i1.05

Spáčil, J. (2024). Attribution of cyber operations: Technical, legal and political perspectives. *International and Comparative Law Review*, 24(2), 150–168. https://doi.org/10.2478/iclr-2024-0022

Sumadinata, W. S. (2023). Cybercrime and global security threats: A challenge in international law. *Russian Law Journal, 11*(3). https://doi.org/10.52783/rlj.v11i3.1112

Tanodomdej, P. (2019). The Tallinn Manuals and the making of the international law on cyber operations. *Masaryk University Journal of Law and Technology, 13*(1), 67–86. https://doi.org/10.5817/MUJLT2019-1-4

Tanodomdej, P. (2019). The Tallinn Manuals and the making of the international law on cyber operations. *Masaryk University Journal of Law and Technology*, 13(1), 67–86. https://doi.org/10.5817/MUJLT2019-1-4

Zheng, Y. (2022). Analysis on the impact of international organizations on international law. In *Proceedings of the 2022 8th International Conference on Humanities and Social Science Research (ICHSSR 2022)* (Advances in Social Science, Education and Humanities Research). Atlantis Press. https://doi.org/10.2991/assehr.k.220504.311