**Evidentiary Standards and Challenges**

# Advantages and Difficulties of Regulating Evidentiary Requirements

## Introduction

The regulation of evidentiary requirements within the context of cyber operations presents a dual-edged sword, offering both significant advantages and formidable challenges. As cyber operations become increasingly prevalent, technologically advanced nations find themselves at the forefront of both executing and defending against such operations. This technological prowess, however, also necessitates a robust framework for attribution, which involves identifying the perpetrators of cyber incidents. The complexity of attribution, compounded by varying international standards and the need for credible evidence, underscores the importance of regulating evidentiary requirements.

At the heart of the debate on evidentiary standards lies the challenge of balancing the need for transparency and accountability with the practical difficulties of gathering and presenting evidence. The lack of uniformity in international law regarding evidentiary standards complicates the attribution process, often leading to political and organizational challenges. This section explores the technological advantages and challenges associated with cyber operations, the intricacies of attribution, and the impact of evidentiary standards on international and domestic legal frameworks.

## Technological Advantages in Cyber Operations

Technologically advanced nations possess a significant advantage in conducting covert cyber operations and attributing cyber incidents. As Rid and Buchanan (2015) argue, the technical prowess and talent pool available to these nations enhance their ability to conceal their operations, uncover others, and respond effectively. This capability allows them to maintain a strategic edge over less technologically equipped adversaries, reversing the assumption that more connected countries are inherently more vulnerable (Rid e Buchanan, 2015, p. 31) .

## Challenges in Attribution

The process of attribution involves multiple layers, each presenting unique challenges that require specific expertise and data. Rid and Buchanan (2015) highlight that attribution does not follow a linear path but rather a cyclical process where new data can reshape existing hypotheses. This complexity necessitates a multidisciplinary approach, combining technical, operational, and strategic analyses (Rid e Buchanan, 2015, p. 9) . Furthermore, attribution is described as an art that relies heavily on skills, resources, and political considerations, making it a nuanced and multi-layered process (Rid e Buchanan, 2015, p. 31) .

Despite the potential for high-quality attribution, limitations such as resource scarcity and time constraints can significantly affect the process. The quality of attribution correlates directly with the resources and time available, posing a challenge even for well-equipped teams when faced with time-sensitive operations (Rid e Buchanan, 2015, p. 32) . Additionally, public attribution requires varying evidentiary standards depending on the action taken, highlighting the complexity of aligning legal and political objectives with technical realities (Grotto, 2020, p. 9) .

### Evidentiary Standards in Attribution

In the context of cyber attribution, evidentiary standards play a crucial role in determining the credibility and effectiveness of attributions. Civil litigation, for instance, demands high evidentiary standards for cyber damage claims, which can influence the outcome of legal proceedings (Grotto, 2020, p. 9) . However, the effectiveness of deterrence may not always be contingent on the evidentiary standards, as strategic communications can serve as a deterrent irrespective of the evidence presented (Grotto, 2020, p. 7) .

Internationally, the lack of consistent evidentiary standards complicates the process of building coalitions against cyber aggressors. The absence of a consensus on what constitutes sufficient evidence under international law poses challenges for states attempting to substantiate their claims (Grotto, 2020, p. 9) . The diversity of conceptions regarding cyber attribution reflects biases and differing evidentiary standards, which can hinder the development of a coherent international framework (Grotto, 2020, p. 2) .

#### International and Domestic Standards

In international armed conflicts, evidentiary standards are crucial for establishing the overall control exerted by sponsoring states over non-state actors. The International Criminal Court has emphasized the need for clear evidence when attributing cyber operations to states, highlighting the challenges posed by ambiguous international law (Hill, 2019, p. 11) . Victim states face significant hurdles in attribution due to the lack of defined terms and thresholds, which complicate the legal response to cyber acts (Hill, 2019, p. 23) .

The absence of clear evidentiary standards under international law further exacerbates the difficulty of attributing cyber operations. While technological advancements aid in identifying physical equipment used in cyber operations, the attribution process requires more than just technical evidence, involving human intelligence and geopolitical considerations (Hill, 2019, p. 23) . The regulation of evidentiary standards could enhance the credibility of attributions, potentially leading to stronger political impacts (Blauth e Gstrein, 2021, p. 8) .

## Conclusion

The regulation of evidentiary requirements in cyber operations presents both opportunities and challenges. Technologically advanced nations have a strategic advantage, yet the complexity of attribution demands a careful balance between technical capabilities and evidentiary standards. The lack of uniformity in international law complicates the attribution process, necessitating a multidisciplinary approach that incorporates technical, political, and legal considerations.

Establishing clear evidentiary standards could enhance the credibility of cyber attributions and foster international cooperation. However, the challenges of resource allocation, time constraints, and geopolitical dynamics must be addressed to ensure effective regulation. As cyber operations continue to evolve, the development of a coherent framework for evidentiary standards will be crucial for maintaining global cybersecurity and accountability.

# Establishment of Evidentiary Rules via Customary International Law

## Introduction

The establishment of evidentiary rules through customary international law plays a crucial role in the global legal landscape, particularly concerning cyber operations and international law. As cyber activities increasingly become a significant aspect of international relations, the need for clear and consistent evidentiary standards has become apparent. These standards are essential for attributing cyber operations and ensuring accountability under international law. The complexity of cyber operations, coupled with the lack of established norms, poses significant challenges for states seeking to hold actors accountable for cyber intrusions.

This section explores the systematic processes of attribution, the challenges of establishing evidentiary standards, and the role of customary international law in shaping these standards. By examining various scholarly perspectives and legal frameworks, we aim to understand how international law can evolve to address the unique challenges posed by cyber operations. The discussion also highlights the importance of credible evidence and the implications of different evidentiary standards on international relations and security.

## Systematic Process of Attribution

The process of attribution in international incidents, particularly those involving cyber operations, follows a systematic approach similar to traditional law enforcement procedures. Rid and Buchanan (2015) describe attribution as an incremental process that begins with the initial report of an incident and progresses through investigation, evidence collection, and ultimately, legal adjudication. This methodical approach underscores the importance of a structured and institutionalized process for determining responsibility, which can be fraught with complexity and drama but remains essential for establishing accountability (Rid e Buchanan, 2015, p. 5) .

## Evidentiary Standards in Cyber Attribution

### International Standards and Challenges

The lack of consistent international evidentiary standards for cyber attribution presents significant challenges. Grotto (2020) notes that there are no consensus standards under international law for assigning blame, particularly in the cyber context. This absence of clear guidelines complicates efforts by states like Americious and Ukaria to build coalitions against cyber aggressors such as Rosaria, as they must persuade other nations of the validity of their attributions without a universally accepted framework (Grotto, 2020, p. 9) . Hill (2019) further elaborates that international law does not outline the necessary evidentiary considerations for cyber operations, highlighting the complexity of attributing such acts due to the lack of uniform rules (Hill, 2019, p. 23) .

Despite these challenges, the variability in evidence provided for attributions can be influenced by international law. Blauth and Gstrein (2021) observe that while providing proof is not mandatory, joint attributions by coalitions of states can enhance legitimacy and political pressure. This variability underscores the importance of policy choices and the potential for states to provide evidence as a means of persuasion rather than obligation (Blauth e Gstrein, 2021, p. 5) .

### Domestic and Civil Litigation Standards

In domestic contexts, evidentiary standards vary significantly, affecting how accusations against foreign governments are handled. Eichensehr (2020) argues that domestic legal standards, such as probable cause for indictments, may be insufficient when accusing foreign governments of cyber misconduct. This discrepancy highlights the need for more robust international standards that can adequately address the nuances of cyber operations and foster the development of norms and customary international law (Eichensehr, 2020, p. 576) .

Greiman (2021) discusses the varying standards of proof required for criminal convictions under U.S. law, noting that these standards differ from those applied in international litigation. This difference emphasizes the need for a harmonized approach that considers both domestic and international legal frameworks (Greiman, 2021, p. 105) .

## Customary International Law and Norms

Customary international law offers a potential pathway for establishing evidentiary standards for cyberattack attributions. Blauth and Gstrein (2021) suggest that while treaties and agreements have faced resistance, customary international law could provide a framework for regulating evidence. This approach relies on consistent and general state practice, coupled with a sense of legal obligation (opinio juris), to crystallize standards of evidence as norms (Blauth e Gstrein, 2021, p. 9) .

However, the current lack of sufficient state practice and opinio juris poses a challenge. Blauth and Gstrein (2021) highlight the need for states to develop more consistent practices, such as agreeing that future public attributions will be substantiated by sufficient evidence. This development would enhance the credibility of attributions and support the evolution of customary international law (Blauth e Gstrein, 2021, p. 9) .

## Conclusion

The establishment of evidentiary rules via customary international law represents a critical step towards enhancing accountability and stability in cyberspace. As cyber operations continue to challenge traditional legal frameworks, the development of clear and consistent evidentiary standards becomes increasingly necessary. By fostering a common understanding of the requirements for attribution, states can improve the credibility of their claims and support the creation of norms that govern state behavior in cyberspace.

While challenges remain, particularly regarding the variability of evidence and the lack of consensus on international standards, the potential for customary international law to provide a framework for these standards offers a promising avenue for progress. As states continue to engage with these issues, the evolution of evidentiary standards will play a crucial role in shaping the future of international law and cyber operations.

# Three Lenses to Interrogate Public Attribution

## Introduction

The concept of public attribution has emerged as a critical component in the strategic landscape of cybersecurity. It involves the public disclosure of the source behind a cyberattack, which can have significant geopolitical and strategic implications. This process of attribution serves multiple purposes, from deterring future attacks to justifying responsive actions on an international stage. However, the decision to publicly attribute a cyberattack involves a delicate balance of technical, political, and legal considerations, each with its own set of challenges and implications.

Public attribution not only influences international relations but also affects domestic politics and corporate strategies. The decision-making process behind public attribution involves assessing the benefits and risks associated with making such information public. This section explores the strategic implications of public attribution, the standards and forms it takes, its impact on domestic and international relations, and the technical and political dimensions that underpin these processes. By examining these aspects, we can better understand the role of public attribution in the broader context of cybersecurity and international diplomacy.

## Public Attribution and Its Strategic Implications

### Forms and Standards of Public Attribution

Public attribution can be seen as a strategic choice that prioritizes the benefits of disclosure over the potential costs associated with selective or private attribution. Grotto (2020) outlines three forms of strategic attribution: private, selective, and public, with public attribution being the most open form of disclosure (Grotto, 2020, p. 6) . The decision to publicly attribute a cyberattack involves calculating that the benefits of such disclosure outweigh the associated costs (Grotto, 2020, p. 8) . This decision-making process also necessitates different evidentiary standards depending on the action being taken, such as criminal indictments or economic sanctions, each with its own requirements (Grotto, 2020, p. 9) .

### Impact of Public Attribution on Domestic and International Relations

Public attribution can generate significant domestic pressure for action against cyber aggressors. The evidentiary standards for public attribution are often context-dependent and politically influenced, lacking the formal safeguards of legal frameworks (Grotto, 2020, p. 9) . Examples of public attribution, such as governmental and corporate responses to cyberattacks, illustrate how these actions can serve as strategic geopolitical interventions (Grotto, 2020, p. 9) . In policy debates, public attribution by states can enhance credibility and defense capabilities, although its effectiveness varies depending on the context (Grotto, 2020, p. 4) .

### Statistical Insights into Public Attribution

Data reveals that a significant majority of cyber incidents result in public attribution, highlighting its prevalence and perceived completeness. According to Kuerbis et al. (2022), 85% of incidents were publicly attributed, indicating a trend towards transparency and accountability in cyber operations (Kuerbis et al., 2022, p. 223) . This trend underscores the importance of public attribution as a tool for both deterrence and accountability.

## Technical and Political Dimensions of Attribution

### Technical Foundations of Attribution

The technical layer forms the foundation of the attribution process, providing the necessary evidence for identifying the perpetrators of cyberattacks. Analysts must efficiently handle a wide range of technical data, from computer code to network activity, which forms the basis for attribution (Rid e Buchanan, 2015, p. 15) . However, the political dimension of attribution complicates the process, as states may employ obfuscation techniques to disguise their involvement, creating a technical race between forensic experts and counter-forensic measures (Kuerbis et al., 2022, p. 223) .

### Risks of Ill-Substantiated Public Attribution

Public attribution carries the risk of being ill-substantiated, especially when driven by political pressures rather than solid evidence. Such attributions can damage reputations and promote irresponsible accusations if not properly substantiated (Yang, 2022, p. 7) . The seriousness of public attribution must match its level of substantiation, as inadequate evidence can lead to international disputes and undermine the credibility of the accusing state (Yang, 2022, p. 3) . Therefore, establishing international norms and standards for public attribution is crucial to ensure responsible and credible accusations (Yang, 2022, p. 7) .

## Legal and Policy Considerations in Attribution

### Legal Frameworks for Attribution

Legal attribution involves connecting offenses to offenders according to domestic or international law. This process legitimizes responsive actions, such as countermeasures, by establishing state responsibility for cyber operations (Yang, 2022, p. 2) . Public attribution plays a crucial role in justifying these actions, as it ensures transparency and accountability on the international stage (Eichensehr, 2020, p. 556) .

### Policy Recommendations for Public Attribution

To minimize disputes, states should engage in consultations before making cyber attributions public. Such consultations can help address substantiation issues and foster cooperation between states (Yang, 2022, p. 8) . The decision-making process for public attribution involves balancing political considerations, such as domestic accountability and international norms, with the need for credible and substantiated claims (Yang, 2022, p. 2) .

## Public Communication and Evidence in Attribution

### Role of Public Communication

Public communication must reflect the probabilistic nature of attribution, acknowledging the mix of fact and judgment involved in the process. Using estimative language can enhance the credibility of public statements by transparently conveying the limitations of current knowledge (Rid e Buchanan, 2015, p. 30) . Public statements and press releases are common tools for attributing cyberattacks, as seen in the U.S. government's responses to incidents like the Sony hack (Eichensehr, 2020, p. 536) .

### Importance of Evidence in Attribution

Publishing detailed evidence can improve the quality of attribution by enabling collective analysis and fostering agreement about state actions. Public disclosure allows for crosschecking by various actors, enhancing the accuracy and credibility of attributions (Rid e Buchanan, 2015, p. 28) . This openness also supports collective defenses against cyber threats by informing other stakeholders about potential risks and mitigation strategies (Rid e Buchanan, 2015, p. 29) .

## International and State-Level Dynamics

### State-Level Challenges and Strategies

Advanced cyber states face a tension between the need for transparency in attribution and the imperative to protect intelligence sources and methods. While transparency can promote mutual restraint and stability, concerns about revealing sensitive information often limit public attributions (Greiman, 2021, p. 106) . However, drawing on nongovernmental information can provide an alternative means of attribution without compromising classified sources (Eichensehr, 2020, p. 569) .

### International Norms and Cooperation

Public attributions supported by evidence can enhance clarity and understanding of state actions, promoting stability in cyberspace. Decentralization of attribution processes allows for a more transparent and timely public disclosure of cyber incidents, fostering international cooperation and reducing the likelihood of conflict (Eichensehr, 2020, p. 556) . This approach encourages a broader range of actors to engage in public attributions, contributing to a more diverse and robust discourse on cybersecurity issues (Eichensehr, 2020, p. 593) .

## Private Sector and Attribution

### Role of Private Firms in Attribution

Private security firms play an increasingly significant role in the attribution landscape, providing valuable public accountability despite their speculative nature. While these firms lack the authority and means for definitive state attribution, their reports offer transparency and relieve governments from the pressure of disclosing sensitive sources and methods (Banks, 2016, p. 1507) . The collaboration between private firms and government agencies strengthens attribution efforts and enhances deterrence against cyber threats (Banks, 2016, p. 1506) .

### Transparency and Accountability

Transparency in state practices is crucial for establishing predictable cybersecurity relations. Public statements about cyber norms and practices contribute to greater stability and predictability by setting clear expectations for state behavior (Banks, 2016, p. 1509) . This transparency helps delineate red lines and reinforces lawful responses, ultimately supporting international law objectives and reducing the risk of cyber conflicts.

## Conclusion

Public attribution serves as a strategic tool that influences both domestic and international landscapes. It involves a careful balance of technical evidence, political considerations, and legal frameworks. While public attribution can enhance transparency and accountability, it also carries risks of ill-substantiation and geopolitical tensions. The role of private firms and the importance of evidence and communication highlight the complexity of attribution processes. As cyber threats continue to evolve, establishing international norms and fostering cooperation among states and private actors will be crucial for effective and responsible public attribution.

# Burden of Proof

## Introduction

The concept of the burden of proof plays a crucial role in legal systems worldwide, determining which party must prove their case and the level of evidence required. In the context of international law and cyber attribution, the burden of proof becomes even more significant due to the complexity of attributing cyber actions to states or non-state actors. The challenges are compounded by the anonymity and low cost of cyber operations, making the establishment of a clear link between actors and actions difficult.

This section explores the intricacies of the burden of proof within international legal frameworks, particularly focusing on cyber attribution and the standards of proof required. It delves into the procedural aspects of burden allocation, the impact of countermeasures, and the varying standards of proof across different legal systems. Additionally, the section examines the practices of international courts, particularly the International Court of Justice (ICJ), and the implications of shifting or reversing the burden of proof.

## State Involvement and Cyber Attribution

### Proof Requirements in Cyber Attribution

Attributing cyber actions to states necessitates proving a relationship between non-state actors and potential perpetrating states. This process is fraught with challenges due to the anonymity and accessibility of cyberspace, which complicates the establishment of such connections. The actions of private citizens are not attributable to states under international law, unless a clear dependency or relationship with the state can be proven (Hill, 2019, p. 11) . The burden of proof typically lies with the claimant state, which must establish responsibility, although proposals for shifting this burden have been suggested, particularly due to the origin state's better access to necessary information (Yang, 2022, p. 6) .

International litigation for cyber disputes reveals varying standards of proof, ranging from prima facie evidence to proof beyond reasonable doubt. These standards reflect the gravity of the charges and the likelihood of the claims being true (Yang, 2022, p. 6) .

### Impact of Countermeasures on Burden of Proof

Countermeasures against a state can alter the burden of proof dynamics. In such cases, the victim state may only need to prove that the origin state failed to prevent significant harm from cyber operations originating within its territory (Greiman, 2021, p. 106) . The complexity of cyber-attack attribution, with its procedural twists, underscores the need for clear legal processes, as highlighted by the International Court of Justice (ICJ), which maintains that the party alleging a fact must prove its existence (Greiman, 2021, p. 105) .

## Standards of Proof in Legal Systems

### Comparative Analysis of Legal Systems

Legal systems across the globe employ different standards of proof. In the U.S., criminal convictions require proof beyond a reasonable doubt, while civil cases may rely on a preponderance of evidence or prima facie standards (Greiman, 2021, p. 105) . The adversarial and inquisitorial systems also differ significantly; the former relies on a competitive process between parties, while the latter involves a more investigative approach by the court (Greiman, 2021, p. 105) .

### Evidentiary Burdens in State Legal Obligations

States often fear that legal requirements for evidence could increase their evidentiary burdens. The "cyber CSI effect" suggests that public expectations for evidence may rise due to nongovernmental attributions, potentially influencing legal standards (Eichensehr, 2020, p. 570) .

## International Court Practices and Burden of Proof

### ICJ and Burden of Proof

The ICJ has consistently held that the burden of proof lies with the party alleging a fact, although the standard of proof remains ambiguous. This lack of clarity has been criticized, as seen in cases like the Oil Platforms and Nicaragua, where the Court did not explicitly define the evidentiary standards required (Eichensehr, 2020, p. 560) . Despite proposals for shifting the burden of proof, the ICJ has historically resisted such changes, maintaining that the party asserting a fact must provide sufficient evidence (Brunner et al., 2019, p. 99) .

### Shifting and Reversing Burden of Proof

Shifting the burden of proof has been proposed as a means to ensure accurate judicial determinations, especially when one party holds exclusive evidence. However, historical precedents like the Corfu Channel case have rejected such shifts, emphasizing the need for states to collaborate in evidence provision (Ronen, 2020, p. 5) (Ronen, 2020, p. 5) . Human rights tribunals, however, have justified burden shifts to address power disparities between states and individuals (Ronen, 2020, p. 6) .

### Standards of Proof and Evidence

The relationship between burden of proof, standard of proof, and evidence is crucial, as these elements are interconnected. The standard of proof serves to protect respondents from false attributions, balancing practicality with the gravity of the breach (Ronen, 2020, p. 21) . The ICJ has been cautious about lowering evidentiary standards, preferring instead to maintain fairness without reversing the burden of proof (Brunner et al., 2019, p. 100) . In cyber contexts, where evidence control can be exclusive, the Court may need to reevaluate its approach (Brunner et al., 2019, p. 98) .

## Conclusion

The burden of proof remains a cornerstone of legal proceedings, ensuring that claims are substantiated with adequate evidence. In the context of international law and cyber attribution, the complexity of proving state involvement necessitates a careful balance between maintaining high evidentiary standards and adapting to the unique challenges posed by cyberspace. While the ICJ and other international bodies have traditionally maintained that the burden lies with the party alleging a fact, there is ongoing debate about the potential need for shifts or adjustments in standards, particularly as cyber operations become more prevalent.

Ultimately, the burden of proof serves not only as a procedural requirement but also as a safeguard against false accusations, ensuring that justice is administered fairly. As legal systems continue to evolve, particularly in response to the challenges of cyber attribution, the principles governing the burden of proof will likely undergo further scrutiny and development.

# The Standard of Proof

## Introduction

The concept of the standard of proof plays a critical role in the legal domain, particularly when determining the responsibility and culpability of parties involved in disputes. In the context of cyber attribution, the standard of proof becomes even more significant due to the complexity and anonymity inherent in cyberspace. This section explores the various evidentiary standards applied in cyber attribution, highlighting the challenges and implications associated with establishing proof of responsibility for cyber operations.

Cyber attribution involves identifying the perpetrators behind cyberattacks, which often requires a robust evidentiary framework. However, the lack of consistent international standards complicates the process, leading to debates on the adequacy and credibility of attributions. This section delves into the nuances of evidentiary standards across different legal contexts and examines their impact on cybersecurity and international relations.

## Evidentiary Standards in Cyber Attribution

### International Standards and Challenges

The lack of consistent international evidentiary standards for cyber attribution presents significant challenges. As noted by Grotto (2020), there are no consensus standards under international law for assigning blame, particularly in the cyber context, which complicates efforts to build multilateral coalitions against malicious actions (Grotto, 2020, p. 9) . Hill (2019) further emphasizes the absence of a uniform body of rules on evidence production, highlighting the complexity of attributing cyber operations due to the varying levels of evidence required (Hill, 2019, p. 23) .

Yang (2022) identifies four levels of proof applicable in international litigation, ranging from prima facie evidence to proof beyond a reasonable doubt, underscoring the variability of standards (Yang, 2022, p. 6) . Banks (2016) notes that international law, as summarized in the Tallinn Manual, requires less proof of attribution than traditional legal expectations, reflecting the unique challenges of cyber operations (Banks, 2016, p. 1510) . Ronen (2020) suggests that different standards of proof should apply based on the legal consequences, advocating for a scale that reflects these differences (Ronen, 2020, p. 12) .

#### Burden of Proof in International Contexts

In cyber attribution cases, the burden of proof typically rests on the claimant state, as highlighted by Yang (2022), who discusses the "virtual control" test tailored for cyber disputes (Yang, 2022, p. 6) . Eichensehr (2020) critiques the International Court of Justice (ICJ) for not explicitly determining the standard of proof required, noting the lack of clarity on evidentiary standards (Eichensehr, 2020, p. 560) . Ronen (2020) points out that international courts often accept circumstantial evidence to address the inequality of proof, allowing for a more liberal recourse to indirect evidence (Ronen, 2020, p. 24) .

### Legal and Procedural Aspects

#### Standards of Proof in Cyber Litigation

Grotto (2020) highlights the high evidentiary standards required for civil litigation involving cyber damage claims, noting that perceived inadequacies can undermine the credibility of accusations (Grotto, 2020, p. 9) . Kuerbis et al. (2022) discuss the procedural challenges of cyber attribution, emphasizing the lack of standardized forensic processes and the reliance on limited evidence (Kuerbis et al., 2022, p. 221) . Yang (2022) underscores the complexity of the burden of proof in cyber-attack attribution, suggesting that shifting the burden may not be effective (Yang, 2022, p. 6) .

Greiman (2021) contrasts adversarial and inquisitorial systems, noting that the burden of proof varies based on the legal system and the nature of the dispute (Greiman, 2021, p. 105) . The ICJ's approach, as discussed by Brunner et al. (2019), requires the same standard of proof for both attribution and violations, emphasizing the need for reasonable certainty (Brunner et al., 2019, p. 97) .

### Impact of Evidentiary Standards on Cybersecurity

#### Enhancing Credibility and Political Impact

Blauth and Gstrein (2021) argue that regulating evidentiary standards could enhance the credibility of cyberattack attributions, leading to stronger political effects (Blauth e Gstrein, 2021, p. 8) . However, establishing such standards requires revealing sources and methods, which can impact state security (Blauth e Gstrein, 2021, p. 7) . Yang (2022) suggests that a "clear and convincing" standard could be appropriate for cyber public attribution, balancing the need for credible evidence with the challenges of disclosure (Yang, 2022, p. 6) .

Greiman (2021) highlights the procedural complexity of cyber-attack attribution, noting that the burden of proof and evidentiary standards are crucial for ensuring accurate judicial determinations (Greiman, 2021, p. 105) . Eichensehr (2020) emphasizes the importance of setting evidentiary standards, arguing that fewer credible attributions are preferable to numerous ill-founded ones (Eichensehr, 2020, p. 6) .

## Unused References

## Conclusion

The exploration of evidentiary standards in cyber attribution reveals a landscape fraught with complexity and inconsistency. The absence of uniform international standards poses significant challenges for states seeking to attribute cyber operations accurately and credibly. The variability of standards across different legal contexts further complicates the process, necessitating a careful balance between the need for credible evidence and the practical challenges of disclosure.

Establishing robust evidentiary standards could enhance the credibility of cyberattack attributions, fostering greater trust and cooperation among states. However, the implications for state security and the potential need for transparency must be carefully considered. As the cyber domain continues to evolve, the development of clear and consistent evidentiary standards will be crucial for ensuring accountability and maintaining international peace and security.

# Means of Proof of Evidence

## Introduction

The concept of evidence and its attribution plays a crucial role in international law, especially when addressing cyber operations and their implications on global security. The complexity of cyber attribution stems from the technical and circumstantial nature of evidence required to substantiate claims. This section explores the various means of proof and evidence, focusing on the challenges and standards involved in attributing cyber activities to specific actors or states.

Attribution of cyber incidents involves a multi-faceted approach, incorporating technical, human, and circumstantial evidence. The process not only requires identifying the perpetrators but also establishing a credible link between the act and the responsible entity. This section delves into the intricacies of attribution, the role of human and state factors, and the standards and burden of proof necessary for substantiating claims within the international legal framework.

## Attribution and Evidence

Attribution of cyber incidents often involves indirect evidence, where connections are suggested rather than explicitly proven. For instance, the speech by America's defense secretary regarding the Shamoon virus attack on Saudi Aramco hinted at Iranian involvement without providing direct evidence, demonstrating how attributions can be interpreted by the international community without concrete proof (Rid e Buchanan, 2015, p. 27) . The ultimate goal of attribution typically focuses on identifying organizations rather than individuals, as illustrated by CrowdStrike's Putter Panda report, which linked a cyber actor's online persona to a specific military unit through various sources of evidence (Rid e Buchanan, 2015, p. 13) .

The credibility of the entity making the attribution significantly influences the persuasiveness of the evidence. Historical instances, such as President Kennedy's assurance to French President de Gaulle during the Cuban Missile Crisis, highlight how reputation can lower the evidentiary burden required for convincing others of a claim (Grotto, 2020, p. 9) . Additionally, timing and the consideration of various factors can enhance the clarity and sufficiency of attribution evidence, emphasizing the need for a robust collection of proof when attributing responsibility for cyber acts (Hill, 2019, p. 22) .

Attribution relies on a diverse array of information sources, including forensics, human intelligence, and circumstantial evidence. These elements collectively form a picture that can link individuals or groups to a particular state, aiding victim states in constructing a credible case for attribution (Hill, 2019, p. 24) .

### Role of Human and State Factors

Proving state involvement in actions by non-state actors requires demonstrating a relationship between the actor and the state. This process can be particularly challenging due to the anonymity and low cost of cyber activities, which complicate the establishment of such connections (Hill, 2019, p. 11) . Human factors, while essential, are part of a broader multidimensional approach that includes assessing the risk and speed of attribution, which are crucial for legitimizing responses to cyber acts (Hill, 2019, p. 22) . In international armed conflicts, evidence of a sponsoring state's overall control over an armed group can internationalize a conflict, necessitating proof of the state's involvement in planning and coordinating military objectives (Hill, 2019, p. 11) .

### Technical and Circumstantial Evidence

Cyber acts require diverse technical means for attribution due to their complexity. Determining responsibility involves multiple levels of attribution, from identifying the equipment used to pinpointing the responsible individuals or groups. This process cannot rely solely on technical means but must also consider the broader context of the act (Hill, 2019, p. 18) . The scarcity of evidence and political motivations can skew the understanding of cyber conflicts, highlighting the importance of transparent and verifiable attributions to prevent false accusations and maintain international norms (Blauth e Gstrein, 2021, p. 6) . Compelling states to provide evidence can prevent wrongful accusations, as seen in the 2015 U.S. claim against China, where the lack of evidence led to disputes over the validity of the attribution (Blauth e Gstrein, 2021, p. 6) .

## Standards and Burden of Proof

The UN Group of Governmental Experts (UNGGE) has emphasized the need for substantiating evidence when attributing cyberattacks, although there is no legal obligation under international law. This highlights the ongoing discussions about establishing clearer standards for evidence (Blauth e Gstrein, 2021, p. 8) . The variability in evidence provided for attributions often depends on policy choices and the influence of international law, with some states opting for more transparency than others (Blauth e Gstrein, 2021, p. 5) . Despite technical challenges, states are encouraged to provide sufficient evidence to substantiate attributions, allowing for crosschecking and enhancing the credibility of claims (Blauth e Gstrein, 2021, p. 10) .

In cyber attribution cases, the burden of proof typically rests on the claimant state, although there are discussions about shifting this burden due to the unique nature of cyber operations. This shift could potentially complicate the attribution process, as the accused state may have better access to necessary information (Yang, 2022, p. 6) . Countermeasures against a state may also influence the burden of proof, requiring the victim state to demonstrate that the origin state failed to prevent harmful cyber operations (Greiman, 2021, p. 106) .

## Evidence in Cyber Operations

The adversarial and inquisitorial systems differ significantly in their approach to establishing proof, with the former relying on a competitive process and the latter on an official inquiry. These differences affect how evidence is gathered and assessed, particularly in the context of cyber operations (Greiman, 2021, p. 105) . In the U.S., varying standards of proof are applied depending on the situation, with the burden of proof being a critical aspect of the attribution process (Greiman, 2021, p. 105) . The challenge lies not only in identifying the source of an attack but also in convincing other states of the accuracy of the attribution, which often involves sensitive intelligence that states may be reluctant to disclose (Greiman, 2021, p. 106) .

Requiring evidence for attributions can improve decision-making and accountability, as seen in U.S. administrative law, where agencies must explain their decisions. This approach could lead to more careful and reasoned attributions, fostering better international cooperation and understanding (Eichensehr, 2020, p. 578) .

## Indirect Evidence and State Responsibility

Relegating evidence-giving to policy risks legitimizing unsubstantiated attributions, which can lead to false claims and exacerbate international tensions. Public attributions supported by evidence can promote stability and understanding, reducing the likelihood of conflict over cyberspace (Eichensehr, 2020, p. 567) . The response to cyber incidents should correlate with the severity of the breach and the available evidence, with more severe breaches requiring greater confidence in the evidence used for attribution (Banks, 2019, p. 195) . However, states are not obligated to provide attribution evidence when responding to cyber intrusions, due to the classified nature of such assessments and the lack of customary international law on the matter (Banks, 2019, p. 195) .

### Case Studies and Analysis

The Russian-Georgian conflict of 2008 provides a rich case study for analyzing indirect evidence of state responsibility for cyber-attacks. This conflict highlighted the use of non-state actors and the reliance on indirect evidence, such as the relationship between the Russian government and national hacker communities, to attribute responsibility (Kadlecová, 2018, p. 38) . The categorization of indirect evidence, although limited, offers a framework for future research and underscores the importance of such evidence in establishing state responsibility (Kadlecová, 2018, p. 43) .

## Legal Frameworks and Evidentiary Standards

International law necessitates a nuanced evaluation of evidence for attribution, considering factors such as reliability, quantum, and specificity. The Tallinn Manual 2.0 provides valuable guidance on these aspects, emphasizing the importance of a granular analysis (Banks, 2016, p. 1508) . States are not required to disclose evidence of attribution, and there are no legal burdens for proof, although the UNGGE suggests that accusations should be substantiated (Banks, 2016, p. 1505) . The ICJ has established principles for assessing evidence, considering factors such as sources, interest, and verification methods, which are crucial for determining the probative value of evidence (Ronen, 2020, p. 23) .

The relationship between burden of proof, standard of proof, and evidence is crucial and interconnected. The ICJ has accepted circumstantial evidence to address inequalities of proof, particularly when direct evidence is unavailable (Ronen, 2020, p. 24) . The standard of proof varies based on the context, with higher standards applied to more serious allegations, ensuring that the respondent is protected against false attribution (Ronen, 2020, p. 8) .

## Challenges in Evidence Gathering

Cyber-attacks often involve scenarios where one party has exclusive control over the evidence, necessitating a reevaluation of evidentiary burdens by the ICJ. The Court may need to shift the burden of proof or rely more on its inherent powers regarding evidence production (Brunner et al., 2019, p. 98) . Bias concerns and outdated perceptions about the necessity of experts hinder effective evidence gathering, highlighting the need for the ICJ to adapt its approach (Brunner et al., 2019, p. 105) . The ICJ has held that circumstantial evidence can support claims if direct evidence is unavailable, setting a threshold of clear and convincing evidence for allegations of unlawful force (Brunner et al., 2019, p. 87) .

The ICJ's standards for evidence need clearer definitions for parties involved in proceedings, ensuring that they are not surprised by the Court's final judgment. The clear and convincing standard balances the need for protection against false attribution with the obligation to prove claims (Brunner et al., 2019, p. 102) . Legal scholars have identified three standards of proof for ICJ cases, with higher standards applied to more serious allegations, ensuring that the burden of proof is appropriately managed (Brunner et al., 2019, p. 89) .

## Conclusion

The means of proof and evidence in cyber operations are critical for establishing accountability and maintaining international security. The complexity of cyber attribution requires a combination of technical, human, and circumstantial evidence, supported by robust legal frameworks and standards. While challenges persist, particularly regarding the burden of proof and the need for transparency, ongoing discussions and advancements in international law aim to address these issues.

Ultimately, the effectiveness of cyber attribution depends on the credibility of the evidence and the willingness of states to adhere to established norms. By fostering cooperation and transparency, the international community can enhance its ability to attribute cyber incidents accurately and respond appropriately, thereby promoting stability and security in cyberspace.

# Evidentiary Issues in the Context of Cyber Operations

## Introduction

In the rapidly evolving landscape of cyber operations, the question of evidence and attribution has emerged as a critical challenge. As cyber threats become more pervasive and sophisticated, the ability to accurately attribute cyber attacks and operations becomes paramount for national security, legal accountability, and international relations. The complexity of cyberspace, characterized by anonymity and the global nature of networks, complicates the process of identifying perpetrators and holding them accountable. This section delves into the evidentiary issues surrounding cyber operations, exploring the challenges and implications of attribution.

The lack of standardized evidentiary processes and the diverse interpretations of international law further complicate the attribution of cyber operations. As states and non-state actors engage in cyber activities, the need for clear and consistent evidentiary standards becomes increasingly apparent. This section will examine the current landscape of evidentiary issues in cyber operations, highlighting the technological, legal, and political challenges that hinder effective attribution and accountability.

## Cyber Operations and Attribution

### Cyber Operations Create New Precedents

The intricacies of cyber operations necessitate a deep understanding of the motivations and behaviors of adversaries. Rid and Buchanan (2015) emphasize that strategic analysis, which includes geopolitical context and the priorities of states, is crucial for understanding the objectives of cyber attacks. This analysis aids in predicting future actions and mitigating potential threats, highlighting the non-technical nature of effective cyber defense strategies (Rid e Buchanan, 2015, p. 25) .

### Attribution Reports Impact Offender Behavior and Operational Decisions

Attribution reports play a significant role in influencing the behavior of offenders. Rid and Buchanan (2015) illustrate how publicizing cyber intrusions can lead to the dismantling of operations, as seen with the rapid shutdown of the Careto operation following Kaspersky Lab's report. The manner of shutdown can provide additional clues about the offenders, such as operational security levels and bureaucratic involvement (Rid e Buchanan, 2015, p. 30) .

### Technologically Advanced Nations Have an Advantage

In the domain of cyber operations, technologically advanced nations often hold a significant advantage. Rid and Buchanan (2015) argue that these nations possess greater technical prowess and talent pools, enhancing their ability to conduct covert operations and uncover those of others. This capability allows them to effectively hide their activities while exposing others, thus reversing the perceived vulnerability of industrialized states (Rid e Buchanan, 2015, p. 31) .

### Public Attribution Necessitates Different Evidentiary Standards

The process of public attribution involves varying evidentiary standards depending on the actions taken. Grotto (2020) discusses how different modalities, such as criminal indictments and economic sanctions, require distinct levels of evidence. The American standard of "beyond a reasonable doubt" for criminal convictions contrasts with the lower standard of "probable cause" for indictments, illustrating the complexity of evidentiary requirements in cyber attribution (Grotto, 2020, p. 9) .

### The Credibility of the Claimant Affects Persuasiveness

The credibility of the entity making an attribution claim significantly influences the persuasiveness of the evidence presented. Grotto (2020) highlights the importance of reputation and integrity, as seen historically when French President Charles de Gaulle accepted the word of the U.S. President without needing further evidence. This underscores the role of trust and credibility in international cyber attributions (Grotto, 2020, p. 9) .

## Evidentiary Standards in Cyber Operations

### Civil Litigation Requires High Evidentiary Standards

In the context of civil litigation, high evidentiary standards are necessary for cyber damage claims. Grotto (2020) notes that alerts on technical threats must withstand scrutiny from skeptics who may challenge the credibility of accusations based on perceived evidentiary inadequacies. This highlights the importance of robust evidence in supporting legal claims (Grotto, 2020, p. 9) .

### Categorizing Attribution for Debate and Standards

Grotto (2020) suggests that categorizing attribution can provide a common reference for scholarly and policy debates, as well as for establishing appropriate evidence standards. This approach aims to enhance clarity and coherence in discussions about cyber attribution, facilitating more informed decision-making (Grotto, 2020, p. 3) .

### International Standards Lack Consistency

There is a notable lack of consistency in international evidentiary standards for cyber attribution. Grotto (2020) points out that unlike criminal proceedings, international affairs lack established rules for evidence, complicating the process of persuading foreign governments of the validity of analytic attributions (Grotto, 2020, p. 9) .

### Regulating Standards Enhances Credibility

Regulating evidentiary standards could enhance the credibility and political impact of cyber attributions. Blauth and Gstrein (2021) argue that while establishing legal requirements may complicate the process, substantiated attributions would likely be more credible and provoke stronger political effects (Blauth e Gstrein, 2021, p. 8) .

### Insufficient State Practice Hinders Norm Establishment

The establishment of customary norms for evidence in cyber attributions is hindered by insufficient state practice and a lack of opinio juris. Blauth and Gstrein (2021) emphasize the need for consistent and general practice among states to develop a more reliable framework for public attributions (Blauth e Gstrein, 2021, p. 9) .

## Unused References

## Conclusion

The evidentiary issues surrounding cyber operations present significant challenges for attribution and accountability. The complexity of cyberspace, coupled with the lack of standardized evidentiary processes and international legal frameworks, complicates the task of identifying and holding perpetrators accountable. As cyber threats continue to evolve, the need for clear and consistent evidentiary standards becomes increasingly crucial. By addressing these challenges, the international community can enhance the credibility and effectiveness of cyber attributions, ultimately contributing to a more secure and stable cyberspace.

# Cyber-Attacks and Evidentiary Difficulties: Estonia and Georgia

## Introduction

The increasing prevalence of cyber-attacks has brought significant challenges to international law, particularly concerning the attribution of such attacks. The cases of Estonia and Georgia serve as poignant examples of the difficulties faced by states when attempting to attribute cyber-attacks and hold perpetrators accountable. These incidents highlight the vulnerabilities of national infrastructures and the complexity of establishing clear evidentiary standards for cyber attribution.

Cyber-attacks, such as the Distributed Denial of Service (DDoS) attacks on Estonia and Georgia, underscore the geopolitical tensions that can exacerbate the challenges of attribution. These cases illustrate the broader issues within international law regarding the lack of consistent evidentiary standards and the reliance on circumstantial evidence. This section explores these challenges, examining the implications of cyber-attacks on international relations and the potential for developing more robust legal frameworks.

## International Evidentiary Standards for Cyber Attribution

The lack of consistent international evidentiary standards for cyber attribution poses significant challenges for states attempting to hold perpetrators accountable. As Grotto (2020) notes, persuading foreign governments of the validity of analytic attributions involves unique challenges due to the absence of consensus standards under international law for assigning blame, particularly in the cyber context (Grotto, 2020, p. 9) . Hill (2019) further elaborates that international law does not outline the necessary evidentiary considerations for cyber attribution, complicating investigations due to the absence of uniform rules on evidence production (Hill, 2019, p. 23) . This lack of clarity allows states to avoid invoking international law when making political attributions, as noted by Blauth and Gstrein (2021), who argue that the law appears weak or irrelevant in holding states accountable for cyber operations (Blauth & Gstrein, 2021, p. 8) .

Despite these challenges, there are discussions about developing standards of proof through customary international law or dedicated cybersecurity treaties. Blauth and Gstrein (2021) suggest that while treaties have been rejected by some states, customary international law could provide a framework for regulating evidence, as violations would be easier to monitor due to the public nature of statements and proofs (Blauth & Gstrein, 2021, p. 9) . This approach could lead to more verifiable and transparent attributions, addressing the current gaps in international law (Blauth & Gstrein, 2021, p. 4) .

### Challenges in Establishing Evidentiary Standards

Establishing evidentiary standards for cyber attribution is crucial for enhancing the credibility of political attributions. Blauth and Gstrein (2021) argue that substantiated attributions could lead to a better understanding of cyberattacks and increase trust, although they acknowledge the challenges posed by the need for states to disclose sensitive information (Blauth & Gstrein, 2021, p. 3) . Yang (2022) supports the idea of setting evidentiary standards, suggesting that fewer credible attributions are preferable to numerous ill-founded ones, even if such standards are not legally required (Yang, 2022, p. 6) .

The ambiguity of international law regarding evidentiary issues allows for reckless cyber attributions, as noted by Yang (2022), who highlights the lack of clear rules or guidelines on evidence, which can be exploited by states (Yang, 2022, p. 5) . Eichensehr (2020) suggests that a mix of existing and new international law may be necessary to address the underdeveloped nature of current evidentiary standards for cyber attribution (Eichensehr, 2020, p. 576) .

### Role of International Law and Organizations

International organizations, such as the UN Group of Governmental Experts (UNGGE), have emphasized the need for substantiating evidence in cyberattack allegations. Blauth and Gstrein (2021) highlight the UNGGE's recommendation that accusations against states should be substantiated, although they acknowledge that this is not a legal obligation (Blauth & Gstrein, 2021, p. 8) . The development of institutional mechanisms and evidentiary standards has been widely debated, with scholars and civil society advocating for guidelines that support reliable public attribution of cyberattacks (Blauth & Gstrein, 2021, p. 4) .

The Atlantic Council's proposal for a multilateral council for adjudicating serious cyberattacks reflects the need for international cooperation and enforcement mechanisms. Such initiatives could draw inspiration from existing international frameworks, like the IAEA or the Biological Weapons Convention, to enhance accountability and trust among states (Kuerbis et al., 2022, p. 231) .

## Public Attribution and Governmental Responses

Public attribution of cyberattacks involves various governmental and corporate responses, as illustrated by examples from Americious and Ukraine. Grotto (2020) describes how Americious government officials publicly attributed a cyberattack to Rosaria, leading to legal actions and economic sanctions (Grotto, 2020, p. 9) . Similarly, Ukraine has publicly attributed numerous cyberattacks to Russia, despite ongoing attacks, highlighting the challenges of attribution and the persistence of cyber threats (Kuerbis et al., 2022, p. 229) .

Selective attribution, as described by Grotto (2020), involves sharing classified threat information with specific stakeholders, such as major grid operators, to manage threat perceptions and encourage information sharing (Grotto, 2020, p. 7) . These examples demonstrate the strategic considerations involved in public attribution and the importance of credible evidence in supporting governmental responses.

## Technical and Legal Challenges in Cyber Attribution

Cyberattack attribution encompasses complex technical, legal, and political dimensions. Eichensehr (2020) notes that while technical attribution has improved, identifying individual perpetrators and states remains challenging due to unsettled legal and political issues (Eichensehr, 2020, p. 523) . Finlay and Payne (2019) highlight the technical challenges of attribution, such as the boundlessness and anonymity of cyberspace, which complicate jurisdiction and enforcement (Finlay & Payne, 2019, p. 203) .

These technical difficulties increase the risk of misattribution, potentially leading to conflict escalation if a state mistakenly targets an innocent third party. The time required for accurate attribution also complicates legal responses, as states may struggle to satisfy the immediacy and necessity required for lawful self-defense (Finlay & Payne, 2019, p. 204) . The difficulty of attributing responsibility for cyberattacks hinders effective legal responses, as states cannot respond without knowing the source of the threat (Finlay & Payne, 2019, p. 202) .

## Evidentiary Standards in Cyber Conflict Scenarios

Cyberattacks can qualify as armed attacks based on their scale and effects, with states considering factors such as severity, immediacy, and military character. Finlay and Payne (2019) discuss the challenges of defining an "armed attack" and the limited number of cyberattacks that meet the necessary threshold (Finlay & Payne, 2019, p. 203) . The Tallinn Manual suggests that acts of cyber intelligence gathering and cyber theft do not meet the threshold of an "armed attack" (Finlay & Payne, 2019, p. 203) .

Addressing the attribution problem in cyberattacks related to armed conflict requires a new model for states. Finlay and Payne (2019) propose a contextually appropriate model for attribution that considers the unique characteristics of cyberattacks and the need for decisive responses (Finlay & Payne, 2019, p. 202) . This approach could enhance the legal framework for addressing cyber armed attacks and improve the effectiveness of international responses.

## State Responsibility and Evidence in Cyber Operations

Establishing state responsibility for cyber operations requires more than just digital evidence. Ronen (2020) argues that digital evidence alone is insufficient due to its volatility and the challenges of collecting it from foreign countries (Ronen, 2020, p. 28) . The collection of evidence may also violate international norms, such as state sovereignty and privacy rights, complicating the admissibility of illegally obtained evidence (Ronen, 2020, p. 28) .

Victim states must prove the affiliation or control of individuals to attribute cyber-attacks to states, as noted by Brunner et al. (2019) (Brunner et al., 2019, p. 94) . The Russian-Georgian conflict provides a case study of indirect evidence suggesting state involvement, highlighting the challenges of proving responsibility without direct evidence (Kadlecová, 2018, p. 43) .

## Cyber-Attacks and Evidentiary Difficulties: Estonia and Georgia

Cyber-attacks on Estonia and Georgia exemplify the challenges of attributing cyber operations and the reliance on circumstantial evidence. Brunner et al. (2019) describe how DDoS attacks targeted Estonian and Georgian infrastructures, with political tensions and Russian IP addresses cited as circumstantial evidence of Russian involvement (Brunner et al., 2019, p. 76) . However, neither Estonia nor Georgia could provide definitive evidence linking the attacks to the Russian government (Brunner et al., 2019, p. 80) .

Circumstantial evidence often remains the only proof available, complicating the attribution process. Brunner et al. (2019) emphasize the difficulty of meeting the "beyond reasonable doubt" standard without compromising sensitive information (Brunner et al., 2019, p. 97) . These cases highlight the need for improved evidentiary standards and international cooperation to address the challenges of cyber attribution.

## Conclusion

The cases of Estonia and Georgia illustrate the significant challenges faced by states in attributing cyber-attacks and establishing accountability under international law. The lack of consistent evidentiary standards and reliance on circumstantial evidence complicate the attribution process, highlighting the need for enhanced legal frameworks and international cooperation. Developing robust evidentiary standards and institutional mechanisms could improve the credibility of cyber attributions and support more effective responses to cyber threats.

As cyber-attacks continue to pose significant risks to national and international security, addressing these challenges becomes increasingly urgent. By exploring new models for attribution and leveraging international law, states can enhance their ability to respond to cyber threats and uphold the principles of accountability and justice in the digital age.

# Evidentiary Standards Before the International Court of Justice

## Introduction

The International Court of Justice (ICJ) plays a crucial role in adjudicating disputes between states, particularly when these disputes involve allegations of wrongful acts such as cyber operations. The evidentiary standards applied by the ICJ are critical for ensuring that justice is served and that states are held accountable for their actions. However, the complexity of cyber operations and the lack of clear international guidelines pose significant challenges for establishing these standards. This section explores the various evidentiary standards employed by the ICJ, the challenges faced in cyber litigation, and the implications for international law and relations.

In the context of cyber litigation, evidentiary standards are particularly contentious due to the technical nature of cyber operations and the difficulty of attributing actions to specific actors. The lack of consistent international standards further complicates matters, as states may have differing expectations and requirements for evidence. This section will analyze the current practices and standards applied by the ICJ and other international bodies, highlighting the need for clearer guidelines and the potential impact on international relations and legal frameworks.

## Evidentiary Standards in Cyber Litigation

The complexity of cyber litigation requires high evidentiary standards, particularly when attributing cyber damage claims. As Grotto (2020) notes, the publication of alerts by Americious ministers on technical threats, while aimed at equipping defenders, often faces skepticism due to perceived evidentiary inadequacies, undermining accusations against Rosaria (Grotto, 2020, p. 9) . This highlights the challenges of meeting evidentiary standards necessary for credible attribution.

Furthermore, the effectiveness of deterrence through attribution signals depends on their credibility and intelligibility. Americious's strategy of selective attribution, as discussed by Grotto (2020), illustrates the delicate balance between public and private signaling required to maintain deterrence without escalating conflicts (Grotto, 2020, p. 7) . The absence of consistent international evidentiary standards complicates these efforts, as noted by Grotto (2020), who points out the lack of consensus on what constitutes sufficient evidence for cyber attributions (Grotto, 2020, p. 9) .

Public attribution involves varying evidentiary standards depending on the action taken, such as criminal indictments or economic sanctions. Grotto (2020) explains that while criminal convictions require evidence beyond a reasonable doubt, indictments and sanctions may operate under lower standards, reflecting the diverse evidentiary expectations across different legal actions (Grotto, 2020, p. 9) . This variability underscores the need for a common reference point for evidentiary standards, as suggested by Grotto (2020), who advocates for categorizing attribution types to facilitate scholarly and policy debates (Grotto, 2020, p. 3) .

## Challenges in Cyber Attribution

The attribution of cyber operations presents numerous challenges, particularly due to the lack of clear international legal standards. Hill (2019) emphasizes that victim states bear the responsibility of proving attribution for international law to apply, yet there are no definitive elements of proof for cyber acts that do not meet the threshold of use of force (Hill, 2019, p. 25) . This ambiguity complicates the application of international law and necessitates further research and collaboration among states.

Moreover, the absence of uniform evidentiary rules for cyber operations complicates investigations, as noted by Hill (2019). The need for clear evidence, as alluded to by the ICJ, remains undefined, leaving states without guidance on the necessary proof for attribution (Hill, 2019, p. 23) . This lack of clarity allows for varying interpretations and practices, which can hinder effective international cooperation and accountability.

## International Law and Cyber Attribution

International law requires that states be held accountable for cyber acts, yet the complexity of attribution poses significant challenges. Hill (2019) discusses the necessity of establishing state culpability for responses to cyber acts, highlighting the difficulty of attributing acts committed by non-state actors without clear guidance from international law (Hill, 2019, p. 12) . This complexity underscores the need for a multidimensional approach that considers technical, legal, and political factors.

The variability in evidence provided for attributions, as discussed by Blauth and Gstrein (2021), reflects the influence of international law on evidentiary standards. While some states provide detailed reports, others rely on political attributions without disclosing evidence, demonstrating the lack of a legal obligation to substantiate claims (Blauth e Gstrein, 2021, p. 5) . This inconsistency highlights the need for clearer standards and guidelines to enhance the credibility and effectiveness of cyber attributions.

## Legal Frameworks and Evidentiary Standards

The establishment of evidentiary standards for cyber attribution is crucial for enhancing the credibility and political impact of attributions. Blauth and Gstrein (2021) argue that regulating evidentiary standards could prevent false accusations and improve trust, although it may require states to disclose sensitive information (Blauth e Gstrein, 2021, p. 3) . This balance between transparency and confidentiality poses a significant challenge for international law.

Yang (2022) suggests that the "clear and convincing" standard should be applied for cyber public attributions, aligning with ICJ practices for self-defense cases (Yang, 2022, p. 6) . This standard, while not as stringent as "beyond reasonable doubt," provides a more robust framework for ensuring that attributions are credible and justifiable.

## International Court of Justice and Evidence

The ICJ's approach to evidence, particularly in cases of exceptional gravity, requires conclusive evidence, as demonstrated in the Genocide Convention case. Eichensehr (2020) highlights that the ICJ demands a high standard of proof for serious allegations, which may be applicable to cyber operations (Eichensehr, 2020, p. 561) . This stringent requirement underscores the importance of establishing clear evidentiary standards for cyber attributions.

However, the ICJ's lack of clarity on evidentiary standards for lower-level actions, as noted by Eichensehr (2020), leaves room for interpretation and inconsistency (Eichensehr, 2020, p. 563) . This ambiguity can lead to challenges in holding states accountable and necessitates the development of more precise guidelines.

## Conclusion

The evidentiary standards employed by the International Court of Justice are critical for ensuring accountability and justice in cases involving cyber operations. However, the lack of clear and consistent guidelines poses significant challenges for states seeking to attribute cyber acts and respond appropriately. The complexity of cyber operations, combined with the absence of uniform international standards, necessitates a multidimensional approach that considers technical, legal, and political factors.

As cyber operations continue to evolve, the need for clearer evidentiary standards becomes increasingly urgent. Establishing robust guidelines will enhance the credibility of attributions, prevent false accusations, and improve international cooperation. By addressing these challenges, the international community can better ensure that states are held accountable for their actions and that justice is served.

# Possible Means to Address the Evidentiary Dilemma in Cyberspace

## Introduction

The advent of cyberspace as a domain of conflict has introduced unique challenges, particularly concerning the attribution of cyber operations and the evidentiary standards required for such attributions. As cyberattacks become more prevalent, the need for robust frameworks that can reliably attribute these attacks becomes paramount. However, the inherent anonymity and complexity of cyberspace complicate the establishment of clear evidentiary standards, leading to significant international legal and political challenges.

This section explores the various dimensions of the evidentiary dilemma in cyberspace, focusing on the standards required for cyber attribution, the role of international law, and the implications for national and international security. By examining scholarly and policy debates, the section aims to provide a coherent narrative that highlights the current challenges and potential solutions for addressing the evidentiary issues associated with cyber operations.

## Evidentiary Standards in Cyber Attribution

The concept of cyber attribution involves various interpretations and biases, reflecting differing evidentiary standards and target audiences. Grotto (2020) highlights the complexity of cyber attribution, noting that while there are commonalities among different conceptions, subtle biases influence the means and ends of attribution, as well as the evidentiary standards applied (Grotto, 2020, p. 2) . This complexity is further compounded by the lack of consistent international evidentiary standards, which presents challenges when persuading foreign governments of the validity of analytic attributions (Grotto, 2020, p. 9) .

Civil litigation also demands high evidentiary standards for cyber damage claims, as seen in the example of Americious, where technical alerts are scrutinized for evidentiary adequacy (Grotto, 2020, p. 9) . However, the effectiveness of deterrence may not be directly influenced by these standards, as selective attribution can serve as a deterrence mechanism without public disclosure (Grotto, 2020, p. 7) . Public attributions, on the other hand, require different evidentiary standards depending on the action, such as criminal indictments or economic sanctions, each with varying levels of proof required (Grotto, 2020, p. 9) .

### International and Legal Perspectives

International law currently lacks clear evidentiary standards for attributing cyber operations, complicating the process of holding states accountable for cyber activities. Hill (2019) discusses the absence of a uniform body of rules for evidence production, highlighting the challenges of attributing cyber operations to a particular state (Hill, 2019, p. 23) . Similarly, Blauth and Gstrein (2021) point out that the lack of clear standards under international law weakens the accountability of states for cyber operations (Blauth e Gstrein, 2021, p. 8) .

Customary international law offers a potential pathway for establishing evidentiary standards, as suggested by Blauth and Gstrein (2021). They propose that consistent state practice and a sense of legal obligation could crystallize as a norm of customary international law, providing a framework for regulating evidence in cyber attributions (Blauth e Gstrein, 2021, p. 9) . However, the ambiguity of international law on evidentiary issues can facilitate reckless cyber attributions, as noted by Yang (2022), who argues that the lack of clear rules allows states to make attributions without consequence (Yang, 2022, p. 5) .

### Public and Political Implications

Establishing evidentiary standards is crucial for enhancing the credibility of political cyberattack attributions. Blauth and Gstrein (2021) emphasize the importance of substantiating attributions with evidence, which can lead to a better understanding of cyberattacks and increase trust among states (Blauth e Gstrein, 2021, p. 3) . Eichensehr (2020) argues that public attributions supported by evidence can promote stability and understanding in cyberspace, reducing the risk of conflict escalation (Eichensehr, 2020, p. 556) .

However, evidence-free attributions can undermine stability, as they may create chaos and increase the risk of conflict among states. Eichensehr (2020) suggests that providing sufficient technical details for corroboration can bolster the credibility of attributions and foster the development of agreed norms or customary international law regarding permissible behavior (Eichensehr, 2020, p. 578) . The establishment of evidentiary standards could thus have a positive impact on international relations and security.

### Technical and Legal Challenges

The collection of evidence for cyber attributions presents significant technical challenges. Blauth and Gstrein (2021) highlight the complexity of the attribution process, which requires multidisciplinary and resourceful teams to overcome technical difficulties (Blauth e Gstrein, 2021, p. 7) . Despite these challenges, states are encouraged to provide sufficient evidence in cyberattack attributions, even if complete certainty cannot be achieved (Blauth e Gstrein, 2021, p. 10) .

Moreover, the reluctance to reveal sources of digital evidence can compromise its acceptance in court, as noted by Ronen (2020). The inability to establish the authenticity and accuracy of evidence may lead to its exclusion or reduced weight (Ronen, 2020, p. 28) . Additionally, collecting evidence for state responsibility may violate international norms, raising questions about the admissibility of illegally obtained evidence (Ronen, 2020, p. 28) .

## Unused References

## Conclusion

The evidentiary dilemma in cyberspace presents a significant challenge for international law and policy, as the lack of consistent standards complicates the attribution of cyber operations. The analysis reveals that while there are efforts to establish evidentiary standards through customary international law and public attributions, significant technical and legal challenges remain. The establishment of clear evidentiary rules could enhance the credibility of attributions, promote stability, and foster the development of international norms regarding cyber behavior.

Ultimately, addressing the evidentiary dilemma requires a collaborative effort among states, international organizations, and the private sector. By developing robust frameworks and leveraging technological advancements, the international community can work towards more reliable and transparent attributions, thereby enhancing global cybersecurity and reducing the risk of conflict.

# The International Law of Evidence

## Introduction

The international law of evidence plays a crucial role in the attribution of cyber operations, a process that involves identifying the responsible parties for cyber incidents. This area of law faces significant challenges due to the unique nature of cyberspace, which often lacks clear evidentiary standards and involves high levels of anonymity and technical complexity. As cyber operations become increasingly prevalent, the need for robust legal frameworks and standards of proof becomes more pressing. This section explores the systematic processes involved in attribution, the challenges faced, and the role of evidence within the context of international law.

Attribution of cyber operations involves a methodical approach similar to traditional law enforcement, where evidence must be meticulously gathered and analyzed. However, the lack of specific international laws regulating cyber-attacks complicates these efforts. This section delves into the systematic processes and challenges of attribution, the role of evidence, and the implications of international law on cyber attribution. By examining these elements, we aim to understand the current landscape and future prospects of international law concerning cyber operations.

## Systematic Process of Attribution

The process of attribution in international law follows a systematic approach akin to traditional law enforcement methods. Rid and Buchanan (2015) describe how attribution unwinds incrementally, beginning with the identification of a crime and progressing through investigation and evidence collection, culminating in a case presented for judgment. This methodical approach, while often dramatic, provides an ordered and institutionalized framework for determining responsibility (Rid e Buchanan, 2015, p. 5) . The ultimate goal of attribution is not merely identifying individuals but linking them to organizations or states, as demonstrated by the case of CrowdStrike's Putter Panda report, which linked a cyber actor to the People's Liberation Army of China (Rid e Buchanan, 2015, p. 13) .

### Challenges in Attribution

Attribution faces numerous challenges, particularly technical ones that complicate evidence collection. Blauth and Gstrein (2021) highlight that the anonymity achievable by attackers and the complexity of cyber forensics make public attribution difficult. Despite advancements, the process remains resource-intensive, requiring multidisciplinary teams to overcome these hurdles and ensure high-quality evidence for political attributions (Blauth e Gstrein, 2021, p. 7) . Furthermore, victim states must navigate ambiguous international laws, which lack defined terms and thresholds, complicating their ability to respond proportionately to cyber acts (Hill, 2019, p. 23) . The absence of specific international laws regulating cyber-attacks further exacerbates these challenges, leaving states without clear guidelines for attribution (Greiman, 2021, p. 102) .

### Role of Evidence in Attribution

The credibility of evidence plays a significant role in the persuasiveness of attributions. Grotto (2020) notes that the reputation of the claimant can affect how evidence is perceived, as seen historically when political leaders accepted evidence based on trust rather than direct proof (Grotto, 2020, p. 9) . States often provide evidence based on policy choices, as seen when attributing cyberattacks to Russian intelligence services, though the level of evidence required remains a matter of choice rather than obligation (Blauth e Gstrein, 2021, p. 5) . The UNGGE has emphasized the importance of substantiating evidence, although there is no legal obligation under international law, highlighting the ongoing discussions about establishing clearer standards (Blauth e Gstrein, 2021, p. 8) .

## International Law and Cyber Attribution

International law currently lacks clear evidentiary standards for attributing cyber operations, posing significant challenges for victim states. Hill (2019) explains that while technology can assist in identifying the physical equipment used, connecting individuals to a state remains difficult due to the anonymity afforded by cyberspace (Hill, 2019, p. 23) . Victim states bear the responsibility of proving attribution, a requirement for international law to apply, yet they face the challenge of undefined proof elements for cyber acts that do not meet the threshold of armed attacks (Hill, 2019, p. 25) . The necessity of establishing state culpability for responses further complicates the process, as international law requires a clear link between the act and the state (Hill, 2019, p. 12) .

### Evidentiary Standards in International Law

The inconsistency of international evidentiary standards for cyber attribution allows for varied interpretations and responses. Grotto (2020) points out that there are no consensus standards for assigning blame, leading to challenges in persuading other states of the validity of attributions (Grotto, 2020, p. 9) . The lack of clear standards facilitates reckless attributions, as states may act without sufficient evidence, exploiting the ambiguity of international law (Yang, 2022, p. 5) . Customary international law could potentially establish standards for evidence, but current state practices lack consistency and generality, hindering the development of such norms (Blauth e Gstrein, 2021, p. 9) .

#### Customary International Law and Evidence

Customary international law offers a potential pathway for establishing evidentiary standards, though its development depends heavily on consistent state practice and a sense of legal obligation. Blauth and Gstrein (2021) suggest that states could agree on providing sufficient evidence for public attributions, which would lead to more consistent practices and eventually crystallize as customary norms (Blauth e Gstrein, 2021, p. 9) . However, the current lack of sufficient state practice and opinio juris presents a significant barrier to establishing such standards (Blauth e Gstrein, 2021, p. 9) .

## Indirect Evidence and State Responsibility

The use of indirect evidence plays a crucial role in attributing state responsibility for cyber-attacks, particularly when direct evidence is lacking. Kadlecová (2018) categorizes indirect evidence from the Russian-Georgian conflict, illustrating how states can be implicated through various forms of indirect proof, such as the level of coordination and preparedness, and relations with national hacker communities (Kadlecová, 2018, p. 38) . This categorization, while limited, highlights the potential of indirect evidence to build a strong attribution case beyond a reasonable doubt (Kadlecová, 2018, p. 42) .

Indirect evidence, such as the collaboration between the Russian government and national hacker communities, provides a compelling case for state involvement, despite official denials and the absence of direct evidence (Kadlecová, 2018, p. 40) . The flexibility of indirect evidence allows for a more nuanced approach to attribution, accommodating the unique challenges of cyberspace where direct evidence may be scarce (Kadlecová, 2018, p. 43) . This approach aligns with the principles outlined in the Tallinn Manual 2.0, which emphasizes the importance of considering the reliability and specificity of available information when determining attribution (Banks, 2016, p. 1508) .

## Conclusion

The international law of evidence concerning cyber operations remains a developing field, characterized by significant challenges and ambiguities. The systematic process of attribution, while methodical, faces hurdles due to the technical complexity and anonymity inherent in cyberspace. The lack of specific international laws and clear evidentiary standards further complicates efforts, leaving states with the responsibility of proving attribution without definitive guidelines.

Indirect evidence emerges as a valuable tool for attributing state responsibility, offering flexibility and adaptability in the absence of direct proof. However, the development of consistent international standards for evidence remains crucial. Customary international law presents a potential avenue for establishing these standards, but requires consistent and general state practice. As cyber operations continue to evolve, the international community must address these challenges, fostering cooperation and clarity in the legal frameworks governing cyber attribution.

# Burden of Proof and Cyber Operations

## Introduction

The evolution of cyber operations has brought about significant challenges and considerations within the international legal framework, particularly concerning the burden of proof and attribution. As cyber operations become more prevalent, the need for accurate attribution becomes critical for determining responsibility and legality. This section explores the intricacies of cyber operations and the burden of proof, examining how these elements intersect with international law and influence global security dynamics.

Attribution in cyber operations involves identifying the source of a cyberattack and assigning responsibility, which can be a daunting task due to the anonymous nature of cyberspace. The burden of proof, traditionally resting on the claimant, becomes a contentious issue as states grapple with the technical and legal challenges of proving cyber intrusions. This section delves into the various standards of proof, the role of international courts, and the implications of shifting the burden of proof, providing a comprehensive overview of the current landscape and the challenges faced by states in navigating cyber operations.

## Cyber Operations and Attribution

### Cyber Operations Create New Precedents

The complexity of cyber operations necessitates a strategic analysis that goes beyond technical aspects, focusing on understanding the motivations and behaviors of adversaries. Rid and Buchanan (2015) emphasize the importance of contextualizing cyber attacks within geopolitical frameworks, which aids in predicting future actions and mitigating breaches (Rid e Buchanan, 2015, p. 25) . This approach highlights the need for a multidisciplinary perspective that integrates geopolitical analysis with technical insights.

### Attribution Challenges

Attribution remains a critical process for assessing responsibility and legality during peacetime cyber operations. Hill (2019) discusses the difficulties of attribution due to the nature of cyberspace, where adversaries can easily deny responsibility (Hill, 2019, p. 4) . This challenge is further compounded when neutral states are implicated due to the interconnected nature of cyber infrastructure.

Victim states must carefully assess the level of responsibility of states involved in cyber operations. Hill (2019) outlines the factors that a victim state must consider, such as the state's ability to detect and enforce prohibitions against hostile acts, which are crucial for determining the extent of responsibility (Hill, 2019, p. 9) .

### The Necessity of Attribution for Self-Defense

The ability to attribute a cyber attack is essential for exercising the right of self-defense. Hill (2019) notes that attribution is critical for both operational and diplomatic responses, underscoring the importance of accurate attribution for maintaining international peace and security (Hill, 2019, p. 3) .

### Imputed Attribution and State Accountability

Imputed attribution holds states accountable for failing to prevent cyber operations originating from their territory. Hill (2019) explains that a state can be held responsible if it consistently fails to impose measures to stop malicious activities, highlighting the importance of proactive measures by states (Hill, 2019, p. 9) .

### Legal Implications of Cyber Operations

The effects of cyber operations play a crucial role in determining the applicability of the law of war. Hill (2019) argues that cyberattacks with effects similar to traditional armed attacks meet the threshold for applying the law of war, emphasizing the need for clear legal frameworks (Hill, 2019, p. 4) .

### Burden of Proof and Cyber Attribution

The burden of proof typically rests on the claimant state in cyber attribution cases. Yang (2022) discusses the potential for shifting the burden of proof, which could complicate the attribution process by establishing prima facie responsibility for the accused state (Yang, 2022, p. 6) . This shift could lead to challenges in ensuring accurate and fair attribution.

There are varying standards of proof in international litigation for cyber disputes, ranging from prima facie evidence to proof beyond a reasonable doubt. Yang (2022) highlights the need for a clear and convincing standard for cyber public attribution, ensuring that evidentiary standards align with the severity of the offense (Yang, 2022, p. 6) .

## Unused References

## Conclusion

The intersection of cyber operations and the burden of proof presents a complex landscape that challenges traditional legal frameworks. As cyber threats continue to evolve, the need for robust attribution mechanisms and clear evidentiary standards becomes increasingly critical. The analysis of cyber operations requires a multidisciplinary approach that integrates technical, legal, and geopolitical insights.

Moving forward, the international community must strive for consensus on attribution standards and burden of proof requirements, ensuring that states can effectively respond to cyber threats while maintaining international peace and security. The development of international norms and legal frameworks will be essential in addressing the challenges posed by cyber operations and ensuring accountability and responsibility among states.

## Introduction

The increasing prevalence of cyber operations has necessitated a reevaluation of traditional legal frameworks and standards of proof, particularly concerning attribution. As cyber operations often transcend national boundaries and involve both state and non-state actors, the complexity of establishing responsibility and legality becomes profound. This section explores the intricacies of cyber operations, focusing on the challenges of attribution and the evolving standards of proof required to hold actors accountable.

Understanding the standards of proof and attribution mechanisms in cyber operations is crucial for maintaining international peace and security. The lack of clear legal guidelines and the rapid evolution of technology pose significant challenges for policymakers and legal practitioners. This section delves into the nuances of cyber attribution, examining the evidentiary standards required and the legal frameworks that govern these operations.

## Cyber Operations and Attribution

### Understanding the Complexities of Attribution

Attribution in cyber operations involves identifying the perpetrators behind cyber attacks, which can be a daunting task due to the technical and geopolitical intricacies involved. Rid and Buchanan (2015) highlight the importance of understanding the adversary's motivation and behavior, which requires a strategic analysis that goes beyond technical aspects. This involves considering geopolitical contexts and the priorities of other states, whether commercial, military, or economic, to contextualize the objectives of a cyber attack and anticipate future actions (Rid e Buchanan, 2015, p. 25) .

Despite the challenges, attribution can debunk the notion of a structural advantage for cyber intruders. Rid and Buchanan (2015) argue that while intruders may have an initial advantage due to the Internet's architecture, a single mistake can expose them through forensic analysis, thereby leveling the playing field for defenders (Rid e Buchanan, 2015, p. 32) . However, the quality of attribution heavily depends on the resources and time available, as highlighted by the limitations discussed by Rid and Buchanan (2015), where high-level decisions may outpace the speed of the attribution process (Rid e Buchanan, 2015, p. 32) .

### Evidentiary Standards and Public Attribution

The evidentiary standards required for public attribution vary depending on the action being taken. Grotto (2020) illustrates that different modalities, such as criminal indictments or economic sanctions, have varying evidentiary requirements. For instance, criminal convictions require a high standard of "beyond a reasonable doubt," whereas economic sanctions may have a lower threshold (Grotto, 2020, p. 9) . This variability underscores the complexity of establishing a uniform standard of proof across different legal and political contexts.

Furthermore, defensive actions may not always require knowing the adversary's identity, as some measures can be implemented based on known technical defenses. However, knowing the adversary can help prioritize mitigation strategies and assess risks more effectively, as discussed by Grotto (2020) (Grotto, 2020, p. 5) .

## Evidentiary Standards in Cyber Operations

### The Need for Clear Standards

International law currently lacks clear evidentiary standards for attributing cyber operations, which complicates investigations among states. Hill (2019) notes the absence of a uniform body of rules on evidence production, making the attribution process reliant on multiple levels of evidence, from identifying physical equipment to proving a state's involvement (Hill, 2019, p. 23) . This gap highlights the need for a multi-dimensional approach that incorporates technological, legal, and political considerations.

Establishing evidentiary standards can enhance the credibility of political attributions, as argued by Blauth and Gstrein (2021). However, such standards require states to disclose their sources and methods, which can impact national security and confidentiality (Blauth e Gstrein, 2021, p. 3) . Despite these challenges, regulating evidentiary standards could lead to more credible attributions and stronger political impacts (Blauth e Gstrein, 2021, p. 8) .

### Challenges and Proposals

Yang (2022) identifies varying standards of proof in international litigation, suggesting that the "clear and convincing" standard may be appropriate for cyber public attributions (Yang, 2022, p. 6) . This standard balances the need for credible evidence with the practical challenges of attribution. However, the burden of proof typically rests on the claimant state, which can complicate the attribution process (Yang, 2022, p. 6) . Eichensehr (2020) proposes a crosschecking requirement as a minimum evidentiary standard, emphasizing the importance of verification for attribution accuracy (Eichensehr, 2020, p. 579) .

## Unused References

## Conclusion

The complexity of cyber operations and the necessity for robust attribution mechanisms underscore the need for clear evidentiary standards. The analysis reveals that while current international law lacks uniform guidelines, there are ongoing efforts to establish credible standards that balance the need for security with the requirement for transparency. The evolving nature of cyber threats necessitates a flexible yet reliable framework that can adapt to technological advancements and geopolitical realities.

Ultimately, enhancing the credibility of cyber attributions through well-defined evidentiary standards can strengthen international cooperation and deter malicious activities. As states continue to grapple with the challenges of cyber attribution, the development of a coherent legal framework will be essential for maintaining global stability and security.

# Methods of Proof and Cyber Operations

## Introduction

The intersection of cyber operations and international law presents a unique challenge, as traditional legal frameworks struggle to adapt to the rapidly evolving cyber landscape. This section explores the methods of proof and the legal implications of cyber operations, focusing on how international law addresses issues of attribution, evidentiary standards, and the use of force. The complexity of cyber operations, characterized by their non-physical nature and the difficulty of attribution, necessitates a reevaluation of existing legal doctrines and the development of new frameworks that can effectively address these challenges.

As cyber operations become increasingly prevalent, they create new precedents and challenge existing definitions of armed attacks. The ambiguity surrounding the attribution of cyber operations and the lack of clear evidentiary standards complicate the application of international law. This section will examine how international law currently addresses these issues, the challenges involved, and potential solutions for improving the legal framework governing cyber operations.

## Cyber Operations and International Law

### Defining Cyber Operations in Legal Contexts

Understanding the rationale behind cyber intrusions is crucial for mitigating future breaches. This involves a strategic analysis that goes beyond technical aspects, requiring a deep understanding of geopolitical contexts and the priorities of other states, whether commercial, military, or economic. Such analysis can provide insights into the objectives of cyber attacks and predict future adversarial actions (Rid e Buchanan, 2015, p. 25) . The Tallinn Manual's Rule 11 establishes that cyber operations can be considered a use of force when their scale and effects are comparable to non-cyber operations, thus applying the Law of Armed Conflict (LOAC) (Hill, 2019, p. 7) . However, existing definitions of armed attacks are challenged by cyber operations, which often have non-physical effects that current international law provisions do not adequately address (Hill, 2019, p. 14) .

### Challenges in Applying International Law

The problem/solution method highlights deficiencies in international law regarding cyber operations, emphasizing the need for a multi-dimensional approach to attribution. This approach must consider both state and non-state actors and address the limitations of current legal frameworks (Hill, 2019, p. 3) . The effects of cyber operations are critical in determining the applicability of the law of war, as cyberattacks that mimic the effects of traditional kinetic attacks meet the threshold of an armed attack (Hill, 2019, p. 4) . However, international law lacks clear evidentiary standards for attributing cyber operations, complicating the process of holding states accountable for cyber acts (Hill, 2019, p. 23) .

## Attribution in Cyber Operations

### Importance of Attribution

Attribution is essential for assessing responsibility and legality in cyber operations. During peacetime, unauthorized access for information gathering may not constitute an attack, but attribution remains critical for any subsequent action (Hill, 2019, p. 4) . The necessity of attribution for self-defense underscores its importance, as states must attribute attacks accurately to exercise their right of self-defense (Hill, 2019, p. 3) .

### Standards and Burden of Proof

International litigation for cyber disputes involves varying standards of proof, ranging from prima facie evidence to proof beyond reasonable doubt (Yang, 2022, p. 6) . The burden of proof typically rests on the claimant state, although a shift of burden has been proposed for cyber attribution, recognizing the origin state's better access to necessary information (Yang, 2022, p. 6) . The "clear and convincing" standard aligns with the adequate level of evidence for cyber public attribution (Yang, 2022, p. 6) .

## Evidentiary Standards in Cyber Operations

### Legal Standards and Proof

Adversarial and inquisitorial systems differ significantly in their approach to establishing proof. The adversarial system relies on a competitive process, whereas the inquisitorial system focuses on pre-trial investigations and interrogations (Greiman, 2021, p. 105) . The burden of proof in cyber-attack attribution remains a complex procedural issue, with the International Court of Justice (ICJ) emphasizing the responsibility of the alleging party to prove their claims (Greiman, 2021, p. 105) . U.S. law illustrates varying standards of proof, from "prima facie evidence" to "beyond reasonable doubt" (Greiman, 2021, p. 105) .

### International Law and Evidentiary Challenges

International law lacks clarity on the standards of proof required for accusations of wrongful acts by states. The ICJ has held that the burden of proof lies with the accusing state, but the specific standard remains undefined (Eichensehr, 2020, p. 559) . The time required for high-confidence attribution can complicate lawful responses, potentially leading to unlawful actions if attribution proves incorrect (Banks, 2019, p. 195) .

## Proxy Operations and State Responsibility

### Legal Implications of Proxy Operations

Proxy operations are often attributed to a state when conducted under its direction or control. This occurs when a state recruits proxies, such as volunteer hackers, to support its cyber operations (Johnson e Schmitt, 2021, p. 21) . However, legal attribution may not be necessary for responding based on necessity, as long as the cyber operation threatens an essential interest of the targeted state (Johnson e Schmitt, 2021, p. 27) . States may act based on necessity even when proxy operations do not violate international law, provided attribution cannot be established (Johnson e Schmitt, 2021, p. 26) .

### State Accountability and Control

A proxy's cyber operation may not violate intervention rules if it lacks coercion, remaining a matter of domestic criminality unless attributable to a state (Johnson e Schmitt, 2021, p. 19) . A state can be held accountable for proxy operations if it acknowledges and adopts the conduct as its own (Johnson e Schmitt, 2021, p. 21) . Proxy operations can also be attributed if conducted by entities dependent on the state, such as intelligence agencies creating unofficial groups for cyber operations (Johnson e Schmitt, 2021, p. 21) .

## Standards of Proof in International Law

### ICJ and Standards of Proof

Legal scholars identify three standards of proof used by the ICJ in cases of state responsibility. These range from "clear and convincing evidence" for regular cases to "beyond reasonable doubt" for cases relying on circumstantial evidence (Brunner et al., 2019, p. 89) . The "clear and convincing" standard effectively balances the need for protection against false attribution with the ability to discharge the burden of proof (Brunner et al., 2019, p. 102) . The ICJ applies the same standard of proof for both attribution and violations, emphasizing the need for reasonable certainty (Brunner et al., 2019, p. 97) .

### Burden of Proof in Legal Proceedings

The burden of proof must be clearly established before determining the standard of proof. The party asserting a fact bears the responsibility of proving it, with the ICJ applying the onus probandi incumbit actori principle (Brunner et al., 2019, p. 83) . This principle underscores the importance of collecting sufficient evidence to support claims, particularly in cases involving violations of international law (Brunner et al., 2019, p. 96) .

## Conclusion

The legal challenges posed by cyber operations necessitate a reevaluation of existing international law frameworks. As cyber operations continue to evolve, they create new precedents and challenge traditional legal definitions, particularly regarding attribution and the use of force. The lack of clear evidentiary standards and the complexity of attribution underscore the need for a multi-dimensional approach that incorporates both technical and legal considerations. By addressing these challenges, the international community can develop more effective legal frameworks that enhance accountability and ensure that states can respond appropriately to cyber threats.

# Presumptions and Inferences in the Cyber Context

## Introduction

The cyber domain presents unique challenges for attribution, the process of identifying the source of a cyber attack. This complexity arises from the technical nature of cyber operations and the geopolitical implications of attribution. The standards and processes for attributing cyber activities are critical for determining the appropriate legal and policy responses. The evidentiary standards required for attribution vary significantly depending on the context and the intended outcome, such as criminal prosecution, economic sanctions, or diplomatic actions. Understanding these standards and the role of presumptions and inferences can help clarify the responsibilities and actions of states and other actors involved in cyber operations.

This section explores the intricacies of evidentiary standards and challenges associated with cyber attribution. It delves into the impact of claimant credibility, the processes involved in attribution, and the normative implications of these processes. Furthermore, the legal and policy frameworks that govern cyber attribution are examined, highlighting the challenges and potential solutions for achieving effective and reliable attribution. By analyzing these elements, we aim to provide a comprehensive understanding of the current landscape and the future directions for cyber attribution.

## Evidentiary Standards and Challenges

### Public Attribution and Evidentiary Standards

The process of public attribution involves varying evidentiary standards depending on the action being pursued. For instance, criminal convictions require a high standard of "beyond a reasonable doubt," while indictments and economic sanctions may operate under lower standards such as "probable cause" or even less stringent criteria. This variability reflects the different stakes involved, from denying personal liberty to imposing economic restrictions (Grotto, 2020, p. 9) . The credibility of the claimant also plays a crucial role; a reputable entity may face a lower evidentiary burden due to its established integrity and honesty, as illustrated by historical diplomatic interactions (Grotto, 2020, p. 9) . Categorizing attribution helps standardize debates and evidentiary expectations across different types of claims, providing a framework for scholarly and policy discussions (Grotto, 2020, p. 3) .

#### Impact of Claimant Credibility

The credibility of the entity making the attribution claim significantly influences the persuasiveness of the evidence presented. Historical examples demonstrate that a strong reputation can reduce the evidentiary burden, as seen when French President Charles de Gaulle accepted the word of the U.S. President without requiring further proof. This underscores the importance of maintaining integrity and trustworthiness on the international stage (Grotto, 2020, p. 9) .

#### Categorization and Common References

By categorizing attribution claims, a common reference point can be established, facilitating more coherent scholarly and policy debates. This categorization aids in setting appropriate evidentiary standards for different types of claims and evaluating the advisability of various proposals aimed at improving attribution practices (Grotto, 2020, p. 3) .

### Attribution Processes and Normative Implications

Attribution involves identifying the attacker, which carries significant normative implications. The process not only assigns blame but also influences the subsequent actions and responses. The act of naming an attacker can serve as a form of coercion or deterrence, impacting international relations and policy decisions (Grotto, 2020, p. 3) . Protagonists often keep their analytic attributions private, drawing from diverse data sources, which can complicate the public attribution process (Grotto, 2020, p. 5) . Analytic attribution relies on both subjective assessments and forensic data, highlighting the challenges of making accurate attributions based on incomplete information (Grotto, 2020, p. 5) .

#### Private Analytic Attributions

Actors involved in cyber attribution often retain their analytic judgments privately, utilizing various data sources. This approach allows for a more controlled and strategic use of information, though it may limit transparency and public accountability (Grotto, 2020, p. 5) .

#### Subjective Assessments in Analytic Attribution

Subjective assessments play a crucial role alongside forensic data in analytic attribution. Decision-makers often rely on incomplete information, making judgments based on intuition and available evidence, which may not always be persuasive to third parties (Grotto, 2020, p. 5) .

## Legal and Policy Frameworks in Cyber Attribution

### State Responsibility and Legal Challenges

The legal framework for cyber attribution involves identifying and assigning responsibility for wrongful acts. The International Law Commission's Draft Articles on State Responsibility provide guidance, emphasizing that states are accountable for cyber activities conducted by their officials, agents, or proxies. This accountability extends beyond technical attribution, requiring a high confidence level before engaging in countermeasures (Banks, 2019, p. 193) . However, states are not obligated to disclose evidence of attribution, complicating the establishment of international norms and practices (Banks, 2016, p. 1505) .

#### Burden of Proof and Evidentiary Thresholds

The burden of proof typically lies with the claimant state, although there are discussions about shifting this burden, especially when the accused state has better access to relevant information. This shift could potentially complicate the attribution process, as establishing prima facie responsibility might lead to unintended consequences (Yang, 2022, p. 6) . In some cases, countermeasures against a state may alter the burden of proof, requiring only proof of a breach of duty rather than direct evidence of attribution (Greiman, 2021, p. 106) .

### International Law and Cyber Operations

Attribution plays a critical role in applying international law, particularly the Law of Armed Conflict (LOAC), to cyber activities. The challenge lies in meeting the evidentiary standards required for self-defense and determining whether a cyber act constitutes an armed attack (Hill, 2019, p. 5) . Imputed attribution holds states accountable for failing to prevent cyber operations from their territory, emphasizing the importance of establishing clear attribution processes (Hill, 2019, p. 9) . During peacetime, attribution remains essential for assessing responsibility and legality, despite the inherent difficulties posed by the nature of cyberspace (Hill, 2019, p. 4) .

#### Human Factors and Circumstantial Evidence

Human factors provide critical circumstantial evidence for cyber attribution. The degree of certainty and the speed of attribution are key variables that influence decision-making and the legitimacy of responses. These factors are not addressed explicitly under international law, highlighting the need for a more nuanced approach (Hill, 2019, p. 22) .

#### Proposed Frameworks and Standards

A due diligence framework has been proposed to establish minimum standards for cyber-attack attribution. This framework emphasizes the responsibility of states to prevent cyber operations from their territory and encourages the development of international norms and standards (Greiman, 2021, p. 107) . Despite extensive literature on cyber attribution, there remains a lack of legal consensus and standards, underscoring the need for continued research and international cooperation (Greiman, 2021, p. 103) .

## Conclusion

In the cyber context, the processes of presumptions and inferences play a crucial role in establishing attribution and determining the appropriate legal and policy responses. The variability of evidentiary standards, influenced by the credibility of the claimant and the intended outcome, highlights the complexity of cyber attribution. Legal and policy frameworks must adapt to these challenges, balancing the need for transparency and accountability with the strategic interests of states.

As cyber operations continue to evolve, the development of international norms and standards becomes increasingly critical. Proposed frameworks, such as due diligence, offer a path forward, but achieving consensus remains a significant challenge. Continued research and international collaboration are essential for enhancing the effectiveness and reliability of cyber attribution, ultimately contributing to a more secure and stable cyber environment.

## Introduction

The concept of inadmissible evidence within the context of international law and cyber operations presents a unique challenge. As cyber threats become increasingly prevalent, the need for robust legal frameworks and evidentiary standards becomes more critical. This section explores the intricacies of evidence attribution, legal obligations, and the challenges faced by international courts when dealing with cyber-related cases. The discussion delves into the nuances of attribution, the role of indirect evidence, and the evolving standards of proof required by international law.

Understanding the dynamics of evidence attribution and its admissibility in international courts requires a multidisciplinary approach. The complexity of cyber operations, coupled with the lack of clear international legal standards, poses significant challenges for states and international bodies. This section aims to provide a comprehensive analysis of the current legal landscape, highlighting the gaps and proposing potential pathways for establishing more effective evidentiary standards.

## Attribution and Evidence

### Sources and Types of Evidence

Attribution of cyber incidents relies heavily on a wide array of information sources, including forensics, human intelligence, and signals intelligence. These diverse sources help construct a picture of the responsible parties and their affiliations, which can be crucial for states seeking to establish accountability for cyber attacks. As Hill (2019) notes, the multidimensional nature of attribution involves analyzing various factors such as past affiliations and associations, which can provide significant leads in identifying perpetrators (Hill, 2019, p. 24) . This approach mirrors traditional law enforcement methods, where circumstantial evidence plays a critical role in building a case.

The timing and additional considerations are also crucial in enhancing the clarity and sufficiency of attribution evidence. Hill (2019) emphasizes the importance of presenting a myriad of evidence to persuade others of a party's responsibility, especially given the lack of clarity under international law for cyber acts below the threshold of warfare (Hill, 2019, p. 22) . These considerations are essential for victim states as they strive to protect their sovereignty and convince international courts of the sufficiency of their evidence.

### Credibility and Persuasiveness

The credibility of the claimant significantly affects the persuasiveness of evidence in international affairs. Grotto (2020) highlights the importance of a claimant's reputation, suggesting that a strong reputation for honesty and integrity can lower the evidentiary burden at the United Nations (Grotto, 2020, p. 9) . This aspect underscores the political dimension of evidence attribution, where the perceived reliability of the claimant can influence the acceptance of evidence, even in the absence of a "smoking gun."

## Legal Obligations and Standards

### Current Legal Framework

The current international legal framework does not recognize a legal obligation for states to provide evidence for attributions. Blauth and Gstrein (2021) argue that the lack of a general sense of legal obligation results in states treating evidence provision as a policy matter rather than a legal requirement (Blauth e Gstrein, 2021, p. 10) . This absence of clear standards complicates the accountability of states for cyber operations, as noted by Finnermore and Hollis, who suggest that the weak role of international law may render it irrelevant in holding states accountable (Blauth e Gstrein, 2021, p. 8) .

### Establishing New Standards

Establishing an international law standard for evidence is crucial for fostering macro-level deterrence and ensuring the credibility of countermeasures. Eichensehr (2020) proposes adopting an evidentiary standard that allows for crosschecking, thereby increasing the deterrent effect of attributions by making countermeasures more credible (Eichensehr, 2020, p. 581) . This approach could facilitate the development of customary international law, as states begin referencing international law in their public statements and attributions (Eichensehr, 2020, p. 584) .

## Challenges in Cyber Attribution

### Technical and Procedural Complexities

The technical challenges associated with cyber attribution are significant, often complicating the collection of evidence. Blauth and Gstrein (2021) discuss the complexity of the forensic process required to uncover the details of cyber attacks, highlighting the role of multidisciplinary teams in overcoming these challenges (Blauth e Gstrein, 2021, p. 7) . Additionally, the procedural aspects of the burden of proof add another layer of complexity, as noted by Greiman (2021), who points out the twists and turns of procedural rules that can hinder the attribution process (Greiman, 2021, p. 105) .

### Convincing Other States

Convincing other states of the accuracy of cyber attribution remains a significant challenge. Greiman (2021) identifies two main reasons for this difficulty: the secretive nature of intelligence-gathering methods and the reluctance to disclose evidence that could help attackers avoid detection in the future (Greiman, 2021, p. 106) . These factors complicate the process of establishing legitimacy for countermeasures and highlight the need for more transparent and robust attribution practices.

## Indirect Evidence in Cyber-Conflicts

### Case Studies and Analysis

The categorization of indirect evidence plays a crucial role in attributing state responsibility for cyber-attacks. Kadlecová (2018) provides an analysis of the Russian-Georgian conflict, identifying four categories of indirect evidence that can be used to attribute responsibility (Kadlecová, 2018, p. 38) . This case study illustrates the challenges of establishing state responsibility, as indirect evidence often serves as the primary means of attribution when direct evidence is lacking (Kadlecová, 2018, p. 37) .

### State Responsibility and Indirect Evidence

Indirect evidence has become increasingly important for attributing responsibility to states for cyber-attacks, especially when non-state actors are involved. Kadlecová (2018) emphasizes the need for states to invoke responsibility and narrow the grey area of accountability by analyzing indirect proofs, which can build a strong case beyond a reasonable doubt (Kadlecová, 2018, p. 42) . This approach underscores the flexibility and necessity of indirect evidence in the absence of direct links between states and cyber-attacks.

## Conclusion

The examination of inadmissible evidence within the context of cyber operations and international law reveals significant challenges and opportunities for establishing more robust legal frameworks. The complexity of attribution, coupled with the lack of clear evidentiary standards, underscores the need for international cooperation and the development of customary international law. By enhancing the credibility of evidence and establishing clear standards, states can improve the effectiveness of cyber deterrence and accountability.

As cyber threats continue to evolve, the role of indirect evidence and the credibility of claimants will become increasingly critical. The international community must work towards creating a cohesive legal framework that addresses the unique challenges posed by cyber operations, ensuring that states can effectively attribute responsibility and protect their sovereignty. This ongoing effort will require collaboration across disciplines and the willingness of states to adapt their practices to meet the demands of the digital age.