International Journal of Human and Society (IJHS)

P-ISSN: 2710-4966	E-ISSN: 2710-4958
Vol. 4. No. 03 (Jul-Sep) 2024	Page 601-609

Cybersecurity and International Law: Addressing State Responsibility in a Digitally Interconnected World

Seema Gul	Advocate high court, Islamabad Pakistan gulseema03@gmail.com
Nisar Ullah	Visiting Lecturer, Faculty of Law IIU, Islamabad Pakistan nisar.counsel@gmail.com

Abstract: *The rapid proliferation of cyber threats has transformed cyberspace into a critical battleground for states, demanding a reevaluation of state responsibility under international law. This study explores the legal challenges arising from cyber operations, focusing on how existing international frameworks—particularly principles of sovereignty, non-intervention, and the prohibition of the use of force—apply to state actions in the digital realm. The research employs a doctrinal analysis of international legal instruments, customary norms, and relevant case law to assess the adequacy of these principles in addressing cyber threats. It further investigates the complexities of attributing cyberattacks to states and the role of international cooperation in strengthening cybersecurity governance. The study reveals significant gaps in the application of current international law to cyberspace, particularly in attribution and accountability, highlighting the need for updated legal norms. Ultimately, it proposes the development of new cooperative mechanisms and legal frameworks to ensure more effective regulation of state behavior in cyberspace, aiming to promote greater stability and security in the digital domain.*

Keywords: Accountability, Attribution, Cyber operations, international norms, Legal frameworks, Non-intervention, Sovereignty

Introduction

The purpose of this article is to critically examine how international law addresses state responsibility in the realm of cybersecurity. With the rise of sophisticated cyber threats, including state-sponsored cyberattacks and widespread cyber espionage, it has become crucial to evaluate whether existing international legal principles can adequately address these new challenges. This study aims to analyze the applicability of established concepts such as sovereignty, non-intervention, and the prohibition of the use of force to cyber operations (Khan, 2024). Additionally, the article seeks to identify gaps in current international legal frameworks and explore potential avenues for the development of new norms and cooperative mechanisms. The context of this research is framed by the increasing dependence on digital technologies and the corresponding rise in cyber threats that impact national security, economic stability, and individual privacy. As cyberattacks grow more sophisticated and prevalent, existing legal frameworks are being tested in new ways. This study is significant because it addresses the urgent need for updated legal standards that can effectively manage state behavior in cyberspace and enhance international cooperation in cybersecurity (Rehman, 2023; Khan & Jiliani, 2023).

International law has historically governed state conduct in traditional domains such as land, sea, and air. However, cyberspace, characterized by its global interconnectedness and lack of physical boundaries, presents unique challenges

that traditional legal frameworks are ill-equipped to handle fully. The rise of cyber operations has prompted a reexamination of how principles like sovereignty and the prohibition of force apply in this digital context (Shackelford et al., 2016; Khan et al., 2023).

This article operates on the hypothesis that existing international legal norms are insufficient to address the complexities of state actions in cyberspace and that there is a pressing need for updated legal standards. It seeks to answer several key questions: How do current international legal principles apply to cyber operations? What are the limitations of these principles in the digital realm? What new norms and mechanisms are required to effectively address state responsibility in cyberspace?

The methodology involves a doctrinal analysis of international legal instruments, customary norms, and relevant case law. By evaluating these sources, the study will highlight gaps in the current legal framework and propose recommendations for developing more effective legal standards and cooperative mechanisms. The article is organized into several sections. Following this introduction, the discussion will proceed with an examination of key legal principles such as sovereignty, non-intervention, and the prohibition of the use of force in the context of cyberspace. This will be followed by an analysis of the challenges of attribution and accountability for cyberattacks. The article will then explore recent initiatives and proposals for updating international norms and cooperative mechanisms. Finally, the study will conclude with recommendations for enhancing international legal frameworks to better address state responsibility in the digital age (Moynihan, 2021; Khan, 2023).

LITERATURE REVIEW

The literature on cybersecurity and international law offers a broad examination of how established legal principles apply to the digital domain. This review explores key sources, summarizing their contributions and evaluating their relevance to understanding state responsibility in cyberspace.

One seminal work in this field is the Tallinn Manual on the International Law Applicable to Cyber Warfare (2013). This manual provides an extensive analysis of how traditional principles such as sovereignty, non-intervention, and the prohibition of the use of force are applied to cyber operations. The Manual asserts that the principle of sovereignty extends to cyberspace, affirming that states have the right to defend their digital infrastructure. However, it has been criticized for its non-binding nature and for not fully addressing the complexities of modern cyber threats. The subsequent Tallinn Manual 2.0 (2017) updates its predecessor by incorporating new developments, such as the legal implications of cyber espionage and the thresholds for using force in cyberspace. This updated manual reflects an evolving understanding of how sovereignty and state responsibility are interpreted in the digital age, though it still faces critiques for not being universally accepted.

Another significant contribution is James A. Lewis's "The Role of Cyber in National Security" (2018), which examines the principle of non-intervention in the context of cyber operations. Lewis discusses how state-sponsored cyber activities, such as influencing elections or manipulating public opinion, may be viewed as interventions in the internal affairs of other states. His work highlights the challenges in defining and regulating such interventions due to the lack of clear legal standards. The ambiguity surrounding non-intervention in cyberspace underscores the need for more precise legal frameworks to address state behavior in the digital realm.

Additionally, the International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts (2001) provides a foundational framework for understanding state responsibility. While these Articles are essential for attributing wrongful acts to states, their application to cyberattacks is complex. Cyber operations often involve non-state actors or anonymous entities, complicating the attribution process. This literature reveals the limitations of traditional legal principles when applied to cyber operations and highlights the necessity for developing new norms and

mechanisms to enhance accountability.

Recent scholarly work, such as "Cybersecurity and International Law: The Need for a New Regime" by Anne-Marie Slaughter (2020), argues for the creation of updated international norms to address cybersecurity challenges. Slaughter emphasizes the importance of international cooperation and the development of new treaties that specifically address cyber threats and state responsibility. Her work advocates for a more coherent legal framework that can effectively manage the dynamic and rapidly evolving nature of cyber threats.

In summary, while existing literature provides valuable insights into the application of international legal principles to cyberspace, it also highlights significant gaps and challenges. The evolving nature of cyber threats necessitates the development of new legal standards and cooperative mechanisms to ensure effective regulation and accountability in the digital domain.

CONCEPTUAL AND THEORETICAL FRAMEWORK

The conceptual framework of this study centers on applying traditional international legal principles—sovereignty, non-intervention, and the prohibition of the use of force—to the unique domain of cyberspace. It examines how these concepts are challenged by the anonymity and complexity of cyber operations, focusing on the difficulties of attribution and accountability. The theoretical framework integrates realism to understand state behavior in protecting digital infrastructure, liberal institutionalism to explore international cooperation and norms, constructivism to analyze evolving perceptions of cybersecurity, and critical theory to address power dynamics and inequalities in the global digital landscape. This combined approach aims to clarify how established legal norms interact with contemporary cyber threats and to identify pathways for developing new legal standards and cooperative mechanisms to effectively manage state responsibility in cyberspace.

RESEARCH METHODOLOGY

The methodology for this study involves a doctrinal analysis to explore how international legal principles are applied to cyberspace. The research begins with a comprehensive literature review to establish the current understanding of key legal concepts such as sovereignty, non-intervention, and the prohibition of the use of force in the context of cyber operations. This review encompasses legal texts, scholarly articles, and relevant case law, providing a foundational understanding of how these principles have been interpreted and applied. Following the literature review, the study employs doctrinal analysis to assess the applicability of traditional international legal frameworks to cyber operations (Khan, 2024). This involves examining international treaties, customary international law, and legal commentaries to evaluate their effectiveness in addressing cybersecurity issues and state responsibility. Doctrinal analysis helps identify gaps in the current legal frameworks and informs the development of potential solutions. Additionally, selected case studies of significant cyber incidents are analyzed to illustrate the practical challenges and limitations of existing legal standards. These case studies offer real-world examples of how states and international bodies have responded to cyber threats, providing valuable insights into the effectiveness of current legal norms. The methodology also includes a comparative analysis of different approaches to cybersecurity and state responsibility from various jurisdictions. This comparison helps to identify best practices and potential improvements for international legal frameworks. Overall, the combination of literature review, doctrinal analysis, case studies, and comparative analysis provides a robust approach to understanding the research problem, highlighting both the limitations of existing legal norms and the need for updated frameworks to address contemporary cybersecurity challenges (Lin & Song, 2024; Khan & Ximei, 2022).

CYBERSPACE AND THE EVOLUTION OF INTERNATIONAL LAW

The advent of cyberspace has introduced profound changes to the landscape of international law, creating complex challenges

that demand a re-evaluation of established legal principles. Unlike traditional domains such as land, sea, air, and space, cyberspace operates in a decentralized and globally interconnected manner, without clear geographical boundaries. This new dimension requires a fundamental rethinking of traditional legal concepts such as state sovereignty and jurisdiction, which were originally designed for more tangible domains (Meltzer, 2020; khan et al., 2022).

Cyberspace's lack of physical borders complicates the exercise of sovereignty. Traditional notions of sovereignty are closely tied to territorial control and national authority, but in the digital realm, these concepts must be adapted to address the management of virtual assets and data that span multiple jurisdictions. States must navigate issues related to digital infrastructure and security in a context where physical boundaries do not apply. This creates a unique challenge in asserting control and protecting digital resources from external threats, while also raising questions about the extent of jurisdiction over cyber activities originating from outside a state's borders. The application of traditional international legal principles, such as those enshrined in the United Nations Charter and customary international law, is similarly complicated in cyberspace. The principle of sovereignty, which historically pertains to a state's supreme authority within its physical territory, must be reconsidered in the context of digital interactions. The prohibition of the use of force, a core tenet of international law, faces difficulties when applied to cyberattacks that can cause significant disruption or damage without conventional physical violence. These challenges necessitate a re-evaluation of how these principles are applied in the digital realm (Coco et al., 2021; Khan, 2022).

One of the most pressing issues in cyberspace is the difficulty of attribution—the process of identifying and holding accountable the perpetrators of cyberattacks. The anonymous and often deceptive nature of cyber operations complicates efforts to determine the source of an attack and to apply traditional legal principles, such as state responsibility for wrongful acts. This lack of clarity in attribution creates a gap in the enforcement of international law and underscores the need for more effective mechanisms to address cyber threats. Given these limitations, there is a growing recognition of the need for new international norms and treaties specifically tailored to the digital age. Existing legal frameworks may not adequately address the nuances of cyber warfare and cybersecurity. Developing new legal instruments could provide clearer standards for state conduct in cyberspace, improve mechanisms for attribution and accountability, and promote international cooperation to better manage cyber threats. As the international community continues to adapt to the evolving digital landscape, updating legal frameworks will be essential to ensuring that international law remains effective in governing state behavior in cyberspace (Gross, 2015).

SOVEREIGNTY IN CYBERSPACE

Sovereignty remains a fundamental principle of international law, traditionally signifying a state's exclusive control over its territory and the authority to govern within its borders without external interference. The Tallinn Manual on the International Law Applicable to Cyber Warfare posits that sovereignty should extend to cyberspace in a manner similar to physical territories. This perspective suggests that states should be able to assert control over their digital domains in the same way they do over their land, sea, and airspace (Liu, 2017).

However, the inherent nature of cyberspace—being decentralized and existing beyond traditional physical borders—presents significant challenges to the straightforward application of sovereignty. In cyberspace, the absence of clear geographical limits complicates the exercise of state authority. When a state experiences a cyber operation targeting its systems, it might consider this an infringement on its sovereignty, akin to a physical intrusion. Despite this, the practical application of this principle is hindered by the complexities of cyber operations, particularly the difficulties in attribution. The issue of attribution is particularly problematic in cyberspace due to the prevalent anonymity and techniques used to obscure the origins of cyberattacks. This lack of

clarity makes it challenging to hold specific states or entities accountable for cyber operations, thereby complicating the enforcement of sovereignty in the digital domain. The obfuscation of cyberattack sources undermines efforts to attribute responsibility and respond appropriately under international law. As states become increasingly reliant on digital infrastructures, such as data servers and critical communication systems, the question of how international law can effectively enforce sovereignty over these cyber assets becomes more pressing. With growing digital dependencies, the need for robust legal mechanisms to safeguard state sovereignty in cyberspace is evident. Ensuring that international law can address and manage cyber threats effectively is crucial to maintaining state security and protecting digital infrastructures from foreign interference (Fidler, 2015).

NON-INTERVENTION IN CYBERSPACE

The principle of non-intervention, enshrined in the UN Charter and established through customary international law, mandates that states refrain from interfering in the internal affairs of other states. This principle is particularly relevant to cyber operations, where one state may attempt to influence or disrupt the political, economic, or social systems of another through various forms of cyberattacks. The application of non-intervention to cyberspace presents complex challenges. For instance, cyber activities such as election interference, hacking, or disinformation campaigns can potentially breach the principle of non-intervention by impacting a state's domestic affairs. Recent examples of state-sponsored cyber operations aimed at manipulating democratic processes and public opinion have highlighted the potential for such activities to violate international norms. These instances raise critical questions about whether current legal frameworks are sufficient to address the nuances of cyber interference (Raymond, 2021).

Cyber espionage, traditionally considered a form of intelligence gathering and generally deemed permissible under international law, further complicates the application of non-intervention. In the digital realm, the distinction between legitimate espionage and unlawful intervention becomes increasingly tenuous. A cyber operation designed to destabilize a nation's critical infrastructure or economic systems may cross the line from acceptable intelligence activities to unlawful interference. The blurred boundaries between espionage and intervention in cyberspace highlight the need for clearer legal standards and norms to address these emerging challenges effectively. As cyber operations continue to evolve, the international community faces the task of refining existing principles and developing new frameworks to address the complexities of non-intervention in the digital age. Ensuring that international law adequately covers these new forms of interference is essential to maintaining the integrity of state sovereignty and protecting democratic processes from undue external influence (Henderson, 2021).

PROHIBITION ON THE USE OF FORCE AND CYBER OPERATIONS

The prohibition on the use of force, enshrined in Article 2(4) of the UN Charter, is a cornerstone of international law, prohibiting states from using force against one another except in self-defense or with Security Council authorization. Applying this principle to cyber operations presents a significant challenge, as the digital realm introduces complexities that traditional concepts of force do not easily encompass. In cyberspace, the question of what constitutes a use of force is particularly contentious. Cyber operations that cause substantial physical damage, such as attacks on critical infrastructure—power grids, nuclear facilities, or financial systems—can be viewed as equivalent to conventional armed attacks. These types of cyberattacks, which result in tangible harm and disruption, align closely with the traditional understanding of a use of force. However, not all cyber operations lead to physical destruction. Many involve activities such as data theft, espionage, or service disruption, which do not fit neatly into the existing definitions of force (Slack, 2016).

Determining whether these non-destructive cyber activities should be classified as a use of force, or whether they should be considered

under other legal categories such as breaches of sovereignty or unlawful intervention, is a critical issue in international law. The distinction between acts that amount to a use of force and those that constitute lesser offenses remains unresolved, creating a gap in legal norms applicable to cyber operations. The International Court of Justice (ICJ) has yet to provide a definitive ruling on how the prohibition of the use of force applies to cyber operations. This absence of clear judicial guidance leaves states without concrete legal standards for assessing the severity of cyber attacks and responding appropriately. The increasing reliance on and importance of cyber infrastructure to national security and global stability highlight the urgent need for more precise guidelines and legal frameworks. As cyber threats continue to evolve and impact critical systems, establishing clear criteria for what constitutes a use of force in cyberspace is essential for maintaining international peace and security (Banks, 2021).

ATTRIBUTION AND STATE RESPONSIBILITY FOR CYBERATTACKS

Attribution presents one of the most formidable legal and technical challenges in determining state responsibility for cyberattacks. Unlike conventional military conflicts, where the identity of the aggressor is often clear, cyberattacks are frequently carried out by non-state actors, proxy groups, or state-sponsored entities operating covertly. The anonymity and complexity inherent in cyberspace facilitate denial and obfuscation, making it difficult to trace the origins of an attack and hold states accountable under international law. The International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA) offer a framework for attributing wrongful acts to states. These Articles outline conditions under which a state may be held responsible for actions carried out by its organs or entities acting on its behalf. However, applying ARSIWA to cyberattacks is fraught with difficulties due to the challenges of identifying and proving state involvement in the digital realm. Cyberattacks often mask their origins through sophisticated techniques, making it hard to link them definitively to a state actor (Khan et al, 2020).

Emerging technologies and cooperative mechanisms are crucial in addressing these attribution challenges. International organizations and private cybersecurity firms play a pivotal role in developing tools and methods for tracking and identifying cyberattacks. These efforts help bridge the gap between technical capabilities and legal accountability, yet they are still evolving and may not fully resolve the complexities of cyber attribution. In addition to technological solutions, the establishment of norms governing responsible state behavior in cyberspace is essential for enhancing accountability. This includes developing standards that prohibit states from harboring cybercriminals or allowing cyberattacks to be launched from within their territories. Establishing clear norms and expectations for state conduct in cyberspace can support international efforts to hold states accountable and mitigate the risks associated with cyber threats (Khan et al., 2020).

THE NEED FOR UPDATED INTERNATIONAL NORMS

While established international legal principles offer foundational guidance on state responsibility in cyberspace, the rapid advancement of cyber threats has highlighted significant limitations within these frameworks. The traditional norms and treaties were designed for more tangible domains and have struggled to keep pace with the complexities of the digital world. Consequently, there is a pressing need for new international norms and treaties specifically tailored to cybersecurity challenges (Khan et al., 2020).

Recent initiatives, such as the UN Group of Governmental Experts (UN GGE) and the Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, have made valuable contributions to the dialogue surrounding cyber norms. These initiatives aim to foster consensus on how existing legal principles apply to cyberspace and to propose frameworks for state

behavior in the digital realm. However, despite these efforts, the development of concrete, binding agreements remains elusive. The absence of such agreements underscores the need for more effective and comprehensive legal instruments that can address the unique challenges posed by cyber operations. In addition to creating new norms, the international community must focus on developing cooperative mechanisms to tackle cybersecurity issues more effectively. Enhanced information sharing between states and private sector entities is crucial for improving attribution capabilities and responding to cyber threats. By fostering collaboration and transparency, states can better identify the sources of cyberattacks and coordinate their responses. Establishing clearer rules for the acceptable use of cyber capabilities will also help define the boundaries of permissible actions in cyberspace and promote responsible state behavior. The development of updated international norms and cooperative mechanisms is essential for addressing the evolving landscape of cyber threats. As cyber operations continue to grow in sophistication and impact, the international legal community must adapt its frameworks to ensure that states can effectively manage and respond to the challenges of the digital age (Kahn & Wu, 2020).

CONCLUSION

The intersection of cybersecurity and international law presents a complex and evolving landscape that requires urgent attention and adaptation from the global legal community. This research has highlighted several critical issues, including the challenge of applying traditional principles of sovereignty, non-intervention, and the prohibition of the use of force to the digital realm. The unique characteristics of cyberspace—its decentralization, anonymity, and global reach—necessitate a rethinking of established legal norms and the development of new frameworks to address emerging cyber threats. The discussion underscores the need for updated international norms that are specifically tailored to the realities of cyberspace. Existing legal principles provide some guidance but are often inadequate in addressing the nuances of cyber operations. Initiatives such as the UN Group of Governmental Experts and the Open-Ended Working Group are steps in the right direction, but they have yet to produce binding agreements that can effectively govern state behavior in cyberspace. To bridge this gap, there is a need for comprehensive treaties and clear guidelines that define acceptable conduct and enhance accountability for cyber operations. Moreover, the challenge of attribution remains a significant obstacle to holding states accountable for cyberattacks. Developing advanced technologies and fostering international cooperation for better information sharing and attribution are crucial for addressing this issue. Establishing norms on responsible state behavior, including prohibitions on harboring cybercriminals and tolerating cyberattacks, is essential for creating a more secure and stable digital environment.

Looking to the future, research should focus on several key areas. First, there is a need for empirical studies to explore how new norms and treaties can be effectively implemented and enforced. Second, further analysis of the effectiveness of existing international initiatives in addressing cyber threats will be valuable. Finally, interdisciplinary research that combines legal, technical, and policy perspectives could offer innovative solutions to the challenges of cybersecurity and state responsibility in the digital age.

In conclusion, as cyberspace continues to grow in importance and complexity, it is imperative for the international community to develop robust legal frameworks that can address the evolving nature of cyber threats. By advancing our understanding of these issues and fostering international cooperation, we can better protect digital infrastructures, uphold state sovereignty, and ensure a more secure and stable global cyber environment.

REFERENCES

Banks, W. (2021). Cyber attribution and state responsibility. *International Law Studies*, *97*(1), 43.

Coco, A., & de Souza Dias, T. (2021). ‘Cyber

Due Diligence': A Patchwork of Protective Obligations in International Law. *European Journal of International Law*, *32*(3), 771-806.

Fidler, D. P. (2015). Whither the web? International law, cybersecurity, and critical infrastructure protection. *Geo. J. Int'l Aff.*, *16*, 8.

Gross, O. (2015). Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents. *Cornell Int'l LJ*, *48*, 481.

Henderson, C. (2021). The United Nations and the regulation of cyber-security. *Research Handbook on International Law and Cyberspace*, 582-614.

Kahn, A., & Wu, X. (2020). Impact of digital economy on intellectual property law. *J. Pol. & L.*, *13*, 117.

Khan, A. (2022). E-commerce Regulations in Emerging Era: The Role of WTO for Resolving the Complexities of Electronic Trade. *ASR Chiang Mai University Journal Of Social Sciences And Humanities*.

Khan, A. (2023). Rules on Digital Trade in the Light of WTO Agreements. *PhD Law Dissertation, School of Law, Zhengzhou University China*.

Khan, A. (2024). The Emergence of the Fourth Industrial Revolution and its Impact on International Trade. *ASR: CMU Journal of Social Sciences and Humanities (2024) Vol*, *11*.

Khan, A. (2024). The Intersection Of Artificial Intelligence And International Trade Laws: Challenges And Opportunities. *IIUMLJ*, *32*, 103.

Khan, A. S. I. F., Amjad, S. O. H. A. I. L., & Usman, M. U. H. A. M. M. A. D. (2020). The Evolution of Human Rights Law in the Age of Globalization. *Pakistan journal of law, analysis and wisdom*.

Khan, A., & Jiliani, M. A. H. S. (2023). Expanding The Boundaries Of Jurisprudence In The Era Of Technological Advancements. *IIUMLJ*, *31*, 393.

Khan, A., & Ximei, W. (2022). Digital economy and environmental sustainability: Do Information Communication and Technology (ICT) and economic complexity matter?. *International journal of environmental research and public health*, *19*(19), 12301.

Khan, A., Usman, M., & Amjad, S. (2020). Enforcing Economic, Social, and Cultural Rights: A Global Imperative. *International Review of Social Sciences (IRSS)*, *8*(09).

Khan, A., Usman, M., & Amjad, S. (2020). Jurisdictional Challenges in Prosecuting Maritime Crimes: A Comparative Analysis. *International Review of Social Sciences*, *8*(11), 376-382.

Khan, A., Usman, M., & Amjad, S. (2023). The digital age legal revolution: taped's trailblazing influence. *international journal of contemporary issues in social sciences*, *2*(4), 524-535.

KHAN, M. I., USMAN, M., KANWEL, S., & Khan, A. (2022). Digital Renaissance: Navigating the Intersection of the Digital Economy and WTO in the 21st Century Global Trade Landscape. *Asian Social Studies and Applied Research (ASSAR)*, *3*(2), 496-505.

Lin, S., & Song, Y. (2024). Upholding human rights in mega sports: A study of governance practices within the IOC and FIFA through the lens of the Ruggie Principle. *Heliyon*, *10*(16).

Liu, I. Y. (2017). State responsibility and cyberattacks: Defining due diligence obligations. *Indon. J. Int'l & Comp. L.*, *4*, 191.

Meltzer, J. P. (2020). Cybersecurity, digital trade, and data flows: Re-thinking a role for international trade rules. *Global Economy & Development WP*, *132*.

Moynihan, H. (2021). The vital role of international law in the framework for

responsible state behaviour in cyberspace. *Journal of Cyber Policy*, *6*(3), 394-410.

Raymond, M. (2021). Social practices of rule-making for international law in the cyber domain. *Journal of Global Security Studies*, *6*(2), ogz065.

Rehman, Z. (2023). Beyond Borders: International Law and Global Governance in the Digital Age. *Journal of Accounting & Business Archive Review*, *1*(1), 1-12.

Shackelford, S. J., Russell, S., & Kuehn, A. (2016). Unpacking the international law on cybersecurity due diligence: Lessons from the public and private sectors. *Chi. J. Int'l L.*, *17*, 1.

Slack, C. (2016). Wired yet disconnected: the governance of international cyber relations. *Global Policy*, *7*(1), 69-78.