DOI: 10.52131/pjhss.2024.v12i1.1977

Pakistan Journal of Humanities and Social Sciences

Volume 12, Number 01, 2024, Pages 271–277
Journal Homepage:
https://journals.internationalrasd.org/index.php/pjhss

# Cyber Law and Cyber Security Policies in Pakistan: A Comparative Study with USA, Canada and Australia

Omer Mahmood Watto[1], Muhammad Islam [2], Syed Arshad Hussain [3], Muhammad Shahab[4]

[1] Ph.D. Scholar, Department of Law, The Islamia University, Bahawalpur, Pakistan. Email: omerwattoo001@gmail.com
[2] Civil Judge-cum-Judicial Magistrate, Lahore High Court, Lahore, Punjab, Pakistan. Email: hsislam786@gmail.com
[3] Civil Judge-cum-Judicial Magistrate, Lahore High Court, Lahore, Pakistan. Email: syedirshadciviljudge@gmail.com
[4] Civil Judge-cum-Judicial Magistrate, Lahore High Court, Lahore, Pakistan. Email: mshahab.rana@gmail.com

**ARTICLE INFO**

***Article History:***
Received: December 19, 2023
Revised: March 04, 2024
Accepted: March 05, 2024
Available Online: March 06, 2024

***Keywords:***
Cyber-security
Cyber-law
Comparative Analysis
Digital Threats
Legal Frameworks
Cybercrime Incidents
Data Protection
National Security
Digital Literacy
Privacy Rights
Cyber Resilience
Global Cyber Landscape
Policy Adaptation

***Funding:***
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

**ABSTRACT**

This study evaluates cyber-law and security policies in Pakistan, the USA, Canada, and Australia, exploring how each country's geopolitical and socioeconomic context influences its cyber-defense and lawful measures against cyber threats. It compares their policies to find out best practices and gaps, aiming to guide the creation of stronger, more adaptable cyber-policies. The research emphasizes the importance of comprehensive legal frameworks to protect against emerging cyber threats and the vital role of international collaboration in enhancing global cyber resilience.



Corresponding Author's Email: hsislam786@gmail.com

## 1. Introduction

In the digital age, the importance of cyber-security and cyber law has increased dramatically due to the pervasive integration of digital technologies into the fabric of daily life and the global economy. The remarkable increase in internet users, coupled with the burgeoning digitalization of services, from banking to healthcare, has rendered cyber law and cyber-security pivotal in safeguarding personal, corporate, and national interests, by establishing legal limitations and security measures against digital threats. These legal frameworks define the rules and regulations governing online actions, data protection, privacy, and intellectual property rights, ensuring users and systems are safeguarded against cybercrimes such as hacking, identity theft, and unauthorized data breaches (Mokalled, Debertol, Meda, & Pragliola, 2017). Together, cyber law and cyber-security create a complete defense structure, ensuring a trustworthy digital environment conducive to economic growth, innovation, and the protection of individual and collective rights in the digital realm. Cyber-security includes the practices, technologies, and processes designed to safeguard networks, computers, programs, and data from attack, damage, or unauthorized access (Poe, 2021). In parallel, cyber law, the legal framework governing internet use and digital transmissions, has evolved to speak to the complex challenges posed by cybercrime, data breaches, and the ethical use of technology. The need for stringent cyber-security practices and thorough cyber law infrastructures has never been more demanding. High-profile cyber-attacks, data breaches, and the misuse of personal data have illuminated the vulnerabilities inherent in the digital world. These events led to real financial damage but also shuddered trust in digital systems and posed a risk to national security (Prakash & Reddy, 2018).

As a result, countries worldwide are striving to strengthen their cyber defenses and legal frameworks to minimize these risks, ensure data privacy, protect intellectual property, and tackle cybercrime. The objectives of this comparative analysis are manifold, Primarily, it seeks to show the evolution, implementation, and challenges of cyber law and cyber-security policies in Pakistan, the USA, Canada, and Australia, providing a panoramic view of how diverse geopolitical and socioeconomic backgrounds shape national cyber-security postures and legal responses to digital intimidations. By dichotomizing the similarities, and variances in methods among these countries, the analysis aims to disclose best practices, identify holes in current outlines, and offer visions that could inform the growth of more effective, hardy, and flexible cyber policies and laws. The countries selected for this comparative study Pakistan, the USA, Canada, and Australia provide a varied range of lookouts due to their diverse cultural, political, and technological landscapes. Pakistan, account, strategic geopolitical location in South Asia, faces unique cyber-security challenges that join with national security and regional balance. The country's growing digital landscape contrasts swiftly increasing internet penetration with emergent cyber law frameworks and cyber-security events.

On the other hand, the USA, as a global skill leader, copes with the dual necessities of furthering innovation and ensuring cyber-security. The intricacy of the American legal system, with its communication of federal and state laws, presents a dynamic set of challenges and opportunities in cyber law and cyber-security policy preparation and application (Hathaway et al., 2012). Canada, known for its vow to privacy and human rights, outfits a nuanced method to cyber-security, balancing distinct freedoms with the need for national security. The country's collective perspective, underlining public-private partnerships, offers valuable visions into collective cyber-security plans. Australia situated in the active Asia-Pacific area, faces quite an infrequent set of cyber-security challenges and opportunities. The country's practical cyber-security policies and legal measures reflect a strategic response to both local needs and regional dynamics, making it an intriguing case in the comparative analysis. By examining these countries, the investigation aims to provide a complete understanding of the worldwide cyber-security and cyber law landscape, proposing valued lessons and strategic visions for legislators, practitioners, and scholars.

## 2. Evolution of Cyber Law and Cyber-security Policies

The growth of cyber law and cyber-security policies across different nations transpires the dynamic chemistry between technological advancements, developing cyber threats, and the responsibility for legal and regulatory frameworks to protect digital spaces. This ancient perspective probes into the developmental routes of cyber law and cyber-security in Pakistan, the USA, Canada, and Australia, highlighting key gages and legislation that have shaped the current background. Throughout the years, Pakistan has been the scene of many high-profile cybercrime incidents, emphasizing the significant challenges the nation confronts in its fight against digital offenses. These incidents have not only had deep social and legal consequences but also heightened the active development of cyber law implementation within the country. Among these, the Axact scandal of 2015 stands out, where a Pakistani IT firm was drawn in operating an wide international diploma fraud, drawing worldwide scrutiny and emphasizing the complex nature of cyber fraud and the sprints in impeaching such crimes that span across borders (Ezell, 2019).

The question of social media harassment has been common with several incidents leading to legal actions that suggest a growing credit of cyber harassment's importance. A prominent example in 2017 involved a Lahore resident sentenced to a significant prison period for the harassment and for blackmailing a woman via Facebook, marking a landmark in legal actions against cyber harassment in Pakistan. The banking sector has not been exempted to cyber threats either, displayed by a spate of ATM skimming frauds, notably in 2018 when an elaborate skimming scheme involving international culprits came to light, prompting a review of cyber-security manners within Pakistani banks (Al Hattali, Hussain, & Frank, 2020). An accused was convicted for cyberstalking through the creation of a fake social media account, In the Sadia Mirza case relating to 2008, registered under the Electronic Transaction Ordinance of 2002, where a legal precedent was set out in addressing such cybercrimes. Hackers managed to steal a considerable sum by exploiting the bank's security vulnerabilities in the Lahore Bank hacking incident reported in 2018, raising alarms about the inefficiency of the security system of Pakistan. These are the instances of cybercrime in Pakistan. Online fraud, and defamation via social media,

demand more comprehensive, effective, and forceful cyber law frameworks to effectively prevent such digital criminal activities.

Journey in cyber law and cyber-security policy was started in Pakistan with the introduction of the *Electronic Transaction Ordinance (ETO) in 2002.* ETO focused at recognizing and facilitating electronic communications and transactions. The Prevention of Electronic Crimes Act (PECA), enactment in 2016 (PECA), was proved a backbone of Pakistan's cyber law framework. PECA addressed the cyber related issues in a wide array of cybercrimes, from cyber terrorism and fraud to cyberstalking and spamming. Procedures and rules for the collection, storage, and transmission of electronic evidence were also devised for the implementation of PECA. Due to the political rivalries, the controversial use of PECA provisions infringed the human rights especially right of privacy and freedom of expression, leading to calls for amendments to ensure the law's balanced application. Some Segments of society in Pakistan are involved in misuse of social media for unethical, immoral, and offensive activities due to ineffective legislation. Despite of all drawbacks, PECA is shaping the evolving landscape of cyber law, revealing the linkage between security needs and human rights (Youn, Kim, Kim, Shin, & Shin, 2018).

The USA is famous in the cyber security laws world-wide and *"Computer Fraud and Abuse Act (CFAA) of 1986"* is the pioneering piece of legislation. Primarily, the CFAA was aimed to combat hacking but later on, its scope was broadened by several amendments to line up with the growing cyber threats. Both federal and state laws characterized the approach of cyber security by creating a legal fabric to address everything from data breaches and privacy protection to cyber terrorism and surveillance. The establishment of *"Department of Homeland Security (DHS) in 2002"*, is a notable one that plays a crucial role in the nation's cyber-security. The sector-specific legislation like the *"Health Insurance Portability and Accountability Act (HIPAA) for healthcare and the GrammLeachBliley Act (GLBA)"* for financial services, highlighting the sectoral approach to cyber-security in the USA (Hathaway et al., 2012).

Canada, has also a predominant position in having a strong cyber law and cyber-security policy framework to secure privacy and data protection, reflective of the country's broader pledge to private rights. The Personal Information Protection and Electronic Documents Act (PIPEDA), 2000, is a basic stair towards privacy protection in the digital age, regulating how private sector organizations gather, and use personal information. Canadian Cyber Security Strategy launched in 2010 is a significant milestone that not only strengthened national strategies but also aimed at enhancing the country's resilience to cyberbullying. This strategy outlined a comprehensive approach to securing government systems, partnering with the private sector, and developing the public's understanding of cyber-security risks. Canada is actively participating in international cyber-security policies, such as the Budapest Convention on Cybercrime, showing its vow to collaborate with global efforts in combating cyber threats.

Australia's cyber-security and cyber-law landscape have undergone a momentous change from a focus on data protection and privacy to a more obvious emphasis on national security. The Privacy Act 1988 has laid the groundwork for data protection, but the mounting cyber threats have yet to lead to more strong national security-driven policies. The Australian Cyber Security Centre (ACSC), 2014, signifies this shift, serving as a centre for government agencies to team up on cybersecurity issues. Global debates have been sped with the implementation of "Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018" due to its potential implications for privacy (Smith & Ingram, 2017). All these legislations and legal frameworks reflect Australia's proactive vision of national security. From the above comparison, it is obvious how developed countries adapt technological advancements to combat rising threats to save the nation.

## 3. Implementation of Cyber-security Policies

Sincere and forceful efforts are the basic requirement for the implementation of cyber-security policies across different nations. These entities apply cyber-security measures in tandem with the private sector to expand the resilience of national cyberinfrastructures. The crucial role of institutions in the cyber-security field within Pakistan, Canada, and Australia need deeper appreciations. Besides NR3C, the Pakistan Telecommunication Authority (PTA) and the Ministry of Information Technology and Telecommunication (MoITT) also contribute to the area of cyber-security by regulating internet and telecommunications and formulating IT guidelines. Public-

private partnerships, in Pakistan's cyber-security implementation, are emerging as a key strategy, with the government engaging with tech companies, and international bodies to enhance cyber resilience The USA boosts a manifold approach to cyber-security, involving numerous federal agencies and institutions. A strong emphasis on public-private partnerships has also played a pivotal role in implementation. The Department of Homeland Security (DHS) is at the front position, coordinating national efforts to enhance resilience and safeguard cyber infrastructure. The National Security Agency (NSA) also plays a substantial role in information assurance and signals intelligence. The Federal Bureau of Investigation (FBI) operates cybercrime investigations more effectively. By working closely with the private sector, the Cybersecurity and Infrastructure Security Agency (CISA), under the DHS, is particularly distinguished for its work to secure the nation's critical infrastructure. These collaborations nurture information sharing and combined cyber-security efforts between the government and private entities.

Canada's cyber-security implementation is illustrated by a coordinated approach that influences the strengths of a variety of agencies, with the Canadian Centre for Cyber Security playing a central role. Established within the Communications Security Establishment (CSE), the Cyber-Centre serves as a unified source of expert advice, and support on cyber security matters for the government, critical infrastructure proprietors, and the public. Public Safety Canada also plays a vital role in national cyber-security, overseeing the implementation of the national strategy and coordinating efforts through different sectors. The combined model extends to partnerships with the private sector and international allies, with initiatives like ' the Canadian Cyber Incident Response Centre' facilitating information sharing and collaboration in cyber-security defense.

Australia's approach to cyber-security is focused on the Australian Cyber Security Centre which integrates cyber-security capacities across government agencies. The ACSC works under the umbrella of the Australian Signals Directorate (ASD) and brings together expertise from the Department of Defense, the Australian Federal Police (AFP), the Australian Security Intelligence Organization (ASIO), and other institutions. Its nationwide initiatives, such as the annual Australian Cyber Security Centre Conference and the ACSC Partnership Program, aim to supplement collaboration between the government and the private-sector. These partnerships are pivotal for sharing threat intelligence, best practices, and strengthening Australia's cyber defenses in a organized manner (Smith & Ingram, 2017). In all these countries, the implementation of cyber-security policies is a multi-layered process that involves a wide range of stakeholders. The institutional frameworks responsible for cyber-security work in tandem with private sector partners to pilot the evolving cyber threat landscape, underscoring the importance of collaboration in achieving cyber resilience.

## 4. Challenges in Cyber Law and Cyber-security

In the sphere of cyber law and cyber-security, nations worldwide grapple with a myriad of challenges that stem from the rapid pace of technological advancements, the borderless nature of the internet, and the growing and strengthening cyber threat landscape. While some of these challenges are universal, others are uniquely shaped by each country's cultural, political context. Common to all countries is the Herculean task of keeping pace with technology. The insistent advancement in digital technologies often outstrips existing legal and regulatory frameworks, leaving gaps that can be exploited by cyber-criminals. International cooperation is another weighty hurdle, as cyber threats frequently create beyond national borders, necessitating cross-border collaborations and coordination that are often hindered by geopolitical tensions and varying levels of cyber capability. In Pakistan, the challenges are compounded by issues like digital literacy which is critical for fostering a cyber-security awareness. The effectiveness of legal enforcement is questioned, given the nascent state of the country's cyber law framework and the limited resources dedicated to cyber-crime units. Cross-border cyber threats are particularly tricky, given the region's complex geopolitical dynamics, necessitating robust international co-operation that is currently in a developmental phase. The USA challenges its unique set of tests, notably the delicate balance between protecting privacy rights and ensuring national security. The Snowden exposes and following debates have emphasized the tensions between administration for security purposes and the right to privacy (Awan, Memon, Shah, & Awan, 2016). The USA's federal structure introduces complexities in cyber law enforcement, with state and federal jurisdictions sometimes at odds, leading to a patchwork of regulations that can perplex entities operating across state lines.

Canada's challenges include bring into line its regulatory frameworks with those of its largest trading partner, the USA, and clinging to the General Data Protection Regulation (GDPR) to smooth trade with the European Union. This regulatory balancing act is hidden by the need to shield Canadian values such as privacy and freedom of expression. Additionally, Canada, like many other nations, faces a shortage of experienced cyber-security professionals, a gap that threatens to weaken the country's cyber-security position. Australia's geopolitical position in the Asia-Pacific plugs its cyber-security challenges with a distinctive sense. Adapting to a rapidly changing cyber-threat landscape is particularly pressing for Australia. It is giving the improving sophistication of cyber-attacks and the emergence of new hazards in the region. The efforts to bolster its cyber defenses must contend with these geopolitical complexities. Despite these challenges, the shared commitment to enhance cyber-security emphasizes the importance of these issues on the global stage (Bello, Jahan, Farid, & Ahamed, 2022). As other countries continue to adopt strategies of each other. The exchange of best practices learned becomes invaluable in forging a more secure and resilient digital world.

## 5. Comparative Analysis

The comparative analysis of cyber law and cyber-security policies across Pakistan, the USA, Canada, and Australia unearths a rich tapestry of approaches. Each reflects the unique sociopolitical and geological backgrounds of these nations (Youn et al., 2018). Despite the diversity in these strategies, common loops emerge, notably in the universal challenges of adapting to rapid technological changes and international cooperation. Pakistan's approach, shaped by its sociopolitical dynamics and regional security concerns, emphasizes rigorous cyber-crime legislation through the Prevention of Electronic Crimes Act (PECA). However, the efforts are being hindered by digital literacy gaps and resource constraints. Digital illiteracy affects the enforcement and public awareness of cyber laws critically. Pakistan critically needs to augment digital literacy and infrastructure to bolster cyber-security measures effectively. The USA has the most advanced technological approaches in all fields, therefore, the approach to cyber-security is also distinguished by its amalgamation of multiple elements that strengthen a strong defense against cyber threats. The USA has cutting-edge technology and a highly developed digital setup. These advanced technological are the base for the implementation of modern security measures and innovations in cyber-defense. The USA has dedicated institutions strong toward combat cyber-security such as the Department of Homeland Security (DHS) and the National Security Agency (NSA). These institutions are working effectively by formulating policies, coordinating national security, and providing guidance on best practices for safeguarding against cyber threats. Several laws and regulations have been enacted by the USA aimed to combat increasing cyber-security threats. Recognizing the importance of a secure digital environment, the USA has made substantial investments in strengthening its cyber setup. This includes funding for establishment of cyber-security research, as well as the enhancement of crucial infrastructure systems' security (Al Qatawneh, Almobaideen, & Qatawneh, 2022). The USA, characterized by its sophisticated technological environment and strong institutional systems.

Canada's approach is characterised by a strong emphasis on data protection, aligning with its democratic values. The Canadian approach, particularly through the Personal Information Protection and Electronic Documents Act (PIPEDA) and its national cyber-security strategy, exposes a commitment to protecting individual rights while ensuring national security. Canada's alignment with international standards, like the GDPR, highlights the status of global interoperability in cyber-security policies. By facing unique geopolitical challenges and promptly evolving threats, Australia's cyber-security policies are marked by its strategic positioning in the Asia Pacific region. Through the establishment of the Australian Cyber Security Centre (ACSC), Australia is making a centralized effort to develop the nation's cyber resilience, focusing on critical infrastructure and national security (Dart & Ahmed, 2023). Australia's recent legislative measures, such as the introduction of the Assistance and Access Act, have glinted global discussions on encoding privacy, highlighting the delicate balance between security and individual freedoms. The aforementioned comparisons reveal both convergence and divergence in the approaches to cyber law and cyber-security. All countries acknowledge the critical importance of cyber-security, and their distinct priorities and challenges. By focusing extensively on national security and critical infrastructure protection, the USA and Australia advanced their technological infrastructures and cyber security policies (Kumar & Panchanatham, 2015). Whereas, Canada puts a greater focus on robust legal structures and the protection of individual liberties. The effectiveness and proficiency of cyber-security policies vary in developed nations like the USA and Australia, which can invest more heavily in cyber-security infrastructure and international

collaborations as compared to underdeveloped countries like Pakistan. Pakistan is making significant strides but faces challenges related to resources, digital literacy, and talent shortages, which can impact the overall effectiveness of its cyber-security measures. Each country's experience is invaluable for introducing future cyber-security strategies globally. Pakistan, the USA, Canada, and Australia offer fertile insights into the diverse strategies nations employ to navigate the complex cyber domain. Every country faces unique challenges such as the global nature of cyber threats and the collective efforts required to tackle them. From each nation's experiences and adapting best practices to regional contexts can substantially enhance global cyber-security position, making the digital world safer for all.

## 6. Suggestion to improve Pakistan's cyber-security landscape

A multidimensional approach is required, to address and improve the cyber security landscape in Pakistan, focusing on legal, technical, and collaborative aspects (Smith & Ingram, 2017). Implementing the following recommendations would mitigate cyber security threats resulting in the enhancement of the overall cyber resilience of Pakistan outlined below:

### 6.1. Legal and Policy Enhancements

A review of existing cybersecurity laws like the Prevention of Electronic Crimes Act (PECA) to address current and emerging cyber threats is SINE-QUA-NON. A comprehensive legal framework should be made to cover aspects like ransomware, and IoT vulnerabilities. Clear Guidelines for Implementation of cyber security policies across different sectors, making sure that these guidelines are practical to the evolving cyber threat setting. Strengthening of international partnerships to get benefits from global best practices and share threat intelligence on cybercrime investigations, adhering to frameworks like the Budapest Convention on Cybercrime (BouSaba, 2019).

### 6.2. Technical Measures

To monitor, detect, and respond to cyber threats in real-time, establishing a robust national cybersecurity infrastructure, including a state-of-the-art national cybersecurity operations center is the need of the time (Trump, 2012). Pakistani IT firms and other allies should encourage the adoption of secure software development practices comprising regular security audits and adherence to international security standards.

### 6.3. Capacity Building and Awareness

To build a skilled workforce capable of tackling cyber threats, invest in cybersecurity education at all levels, from IST steps to professional training programs. Launching of nationwide public awareness campaigns to raise public awareness about cyber hygiene practices. Develop Cybersecurity Professionals: Through scholarships, internships, and career development programs should be launched to foster the development of cybersecurity professionals in cooperation with the private sector and international partners.

### 6.4. Collaboration and Partnership

To conduct cutting-edge cybersecurity research and partner with universities and research institutions. Engaging in international cyber security forums and working groups to stay abreast of global cyber trends and threats.

### 6.5. Incident Response and Management:

To swiftly manage and mitigate cybersecurity incidents across the nation establishment of a dedicated national incident response team is direly needed. To test and improve the country's incident response capabilities it is required to conduct regular national cybersecurity exercises simulating various cyber-attack scenarios. By applying the above-mentioned recommendations, Pakistan can considerably enhance its cybersecurity posture to a safer global system.

## 7. Conclusion

Pakistan, the USA, Canada, and Australia’s comparative study, on cyber-law and security policies, concludes that each country's approach is deeply influenced by its unique geopolitical and socioeconomic context. There are also universal propositions in the investigation of a secure digital environment. This study highlights the importance of comprehensive legal frameworks and forceful cyber-security measures to protect against the ever-evolving settings of digital threats. It points out the complexities of individual privacy rights and balancing national security,

within the digital era protectively. It further divulges from this comprehensive analysis that, common challenges such as rapid technological advancements, international cooperation, and the need for a skilled cyber-security workforce persist yet. The USA's emphasis, on public-private partnerships and advanced technological infrastructure, identifies the best practices for the protection of cyber resilience. Canada's focus on privacy and alignment with international standards is the best model for cyber protection. Australia's strategic response to regional dynamics is also an endeavour to safeguard cyber security vulnerability. According to regional contexts and prevailing issues, the indispensable role of international cooperation in enhancing global cyber resilience has become the need of the day. The study further advocates for the adaptation of these best practices. In conclusion, the research offers valued insights for policymakers, practitioners, and scholars. To sum up, the article suggests that a combination of adaptable legal measures, strategic international partnerships, and continuous investment in cyber-security substructure is essential for creating a safer global digital world.

**References**


Al Hattali, S. S. K., Hussain, S. M., & Frank, A. (2020). Design and development for detection and prevention of ATM skimming frauds. *Indonesian Journal of Electrical Engineering and Computer Science, 17*(3), 1224. doi:https://doi.org/10.11591/ijeecs.v17.i3.pp1224-1231

Al Qatawneh, I. S., Almobaideen, W., & Qatawneh, M. (2022). A comparative study on surveillance and privacy regulations (The UAE vs. the USA and the EU).

Awan, J. H., Memon, S., Shah, M. H., & Awan, F. H. (2016). *Security of eGovernment services and challenges in Pakistan.* Paper presented at the 2016 SAI computing conference (SAI).

Bello, A., Jahan, S., Farid, F., & Ahamed, F. (2022). A Systemic Review of the Cybersecurity Challenges in Australian Water Infrastructure Management. *Water, 15*(1), 168. doi:https://doi.org/10.3390/w15010168

BouSaba, C. (2019). *Implementing a DeMilitarized Zone Using Holistic Open Source Solution.* Paper presented at the 2019 ASEE Annual Conference & Exposition.

Dart, M., & Ahmed, M. (2023). CYBER-AIDD: A novel approach to implementing improved cyber security resilience for large Australian healthcare providers using a Unified Modelling Language ontology. *Digital Health, 9*, 20552076231191095. doi:https://doi.org/10.1177/20552076231191095

Ezell, A. (2019). Academic Fraud and the World's Largest Diploma Mill. *College and University, 94*(4), 39-46.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California law review*, 817-885.

Kumar, D., & Panchanatham, N. (2015). A case study on Cyber Security in E-Governance. *International Research Journal of Engineering and Technology (IRJET), 2*(8), 272-275.

Mokalled, H., Debertol, D., Meda, E., & Pragliola, C. (2017). *The importance to manage data protection in the right way: problems and solutions.* Paper presented at the Optimization and Decision Science: Methodologies and Applications: ODS, Sorrento, Italy, September 4-7, 2017 47.

Poe, L. (2021). Cybercrime in the Age of Digital Transformation, Rising Nationalism and the Demise of Global Governance. *Modern Police Leadership: Operational Effectiveness at Every Level*, 109-126. doi:https://doi.org/10.1007/978-3-030-63930-3_11

Prakash, K. B., & Reddy, P. S. (2018). Cyber laws and cyber security: The jurisprudence and judicature. *Indian Journal of Computer Science, 3*(6), 20-24. doi:http://dx.doi.org/10.17010/ijcs%2F2018%2Fv3%2Fi6%2F141445

Smith, F., & Ingram, G. (2017). Organising cyber security in Australia and beyond. *Australian Journal of International Affairs, 71*(6), 642-660. doi:https://doi.org/10.1080/10357718.2017.1320972

Trump, I. (2012). Confronting the legal liabilities of IT Systems. *EDPACS, 46*(2), 11-16. doi:https://doi.org/10.1080/07366981.2012.682535

Youn, H., Kim, D., Kim, Y.-H., Shin, D., & Shin, D. (2018). *System Information Comparison and Analysis Technology for Cyber Attacks.* Paper presented at the Advances in Computer Science and Ubiquitous Computing: CSA-CUTE 17.