Public Management and Operations Review (PMOR)

Volume 1 Issue 1, Fall2025

Homepage: https://journal.vu.edu.pk/PMOR

ISSN: Online (3106-8057) – Print (3106-8057)

Title: Prioritizing Cyber-Security Measures for Pakistan National Government Websites: A Strategic Assessment of Governance and International Cooperation

Author (s): *Doha, Muqarrab Akbar* *

Affiliation (s): Department of Political Science, Bahauddin Zakaria Univesity, Multan, Pakistan

Corrospendance: Muqarrab Akbar muqarrabakbar@bzu.edu.pk

A Publication Of
Department of Public Administration
Virtual University of Pakistan, Islamabad

Prioritizing Cyber-Security Measures for Pakistan National Government Websites: A Strategic Assessment of Governance and International Cooperation

Abstract:
The paper will discuss the increasing cyber threats to Pakistani national websites through the assessment and prioritization of governance-based and international cooperation-based cybersecurity interventions through the ISM-MICMAC methodology. Pakistan is in urgent need of an organized and comprehensive defense approach, beyond technical solutions alone, since there have been more than 1,500 government-targeted attacks in year 2024. The ISM model initially identifies twelve major measures, and it is hierarchically organized with the base of it being the foundational factors, including a 'National Cyber Security Strategy' and 'Cyber Security Governance Framework'. These factors drive measures including 'managing Incident Response Coordination' and 'Cyber Security Auditing'. MICMAC analysis also categorizes measures based on driving power and dependence and the result is Secure Software Development Lifecycle (SDLC) as one of the most important interventions. International collaboration and sharing of threat intelligence becomes an imperative enabler. It is the first study to use ISM-MICMAC to cybersecurity governance in Pakistan, which provides practitioners and policymakers with a prioritized actionable roadmap. The study helps to efficiently distribute the resources on improving the national digital infrastructure by elucidating interdependencies between the strategic and operational responses to emerging cyber threats. The results can be used to make scholarly and practical contributions to cybersecurity resilience in developing economies where the issues are similar.

Keywords: *Cybersecurity; Pakistan; ISM-MICMAC; Governance; International Cooperation; National Websites; Cyber Threats; Policy Prioritization.*

1. Introduction

Cyber security is one of the most urgent issues today for the world as the number and sophistication of cyber attacks has reached a dangerous level where national security, economic stability and safety can all be at stake (Dutta et al., 2022). The International Telecommunication Union (ITU) in 2020 reported that cybercrime costs globally will exceed $10 trillion per year by 2025 (El-Moghazi & Whalley, 2022). States all over the world are struggling with increased number of cyberattacks such as ransomware, breaches and cyber espionage. The case in Pakistan is just as worrying, with cyber attacks on government websites, critical infrastructure and private sectors growing significantly. As per the Pakistan Cyber Incident Response Centre (PCIRC), more than 1,500 cyberattacks against government websites in this year alone, we urgently require effective cyber security solutions to safeguard the nation's digital infrastructure (Watto et al., 2024).

With this increase in cyber threats, several measures have been taken around the world to safeguard digital assets. Good cyber security solutions generally contain a mix of technological, organizational and policy solutions. These usually include governance, global security standards compliance, employee training, disaster mitigation and sector collaboration. International cooperation, for example the European Union Agency for Cybersecurity (ENISA), has helped share threat information, work out shared protocols and improve cross-border defences (Bederna & Rajnai, 2022). For Pakistan's national websites, a unified approach that encompasses both governance arrangements and global cooperation could help in significantly improving the country's cyber

defences.

Though cyber security's significance has been recognized as an increasing area, there is still research missing on how governance and global co-operation-based countermeasures could be put into practice in Pakistan. Though some of these articles Jawhar et al. (2024) have been conducted in the global context of cyber security measures, none have focused on the use of these measures in the Pakistani state. Only a handful of articles Ajiga et al. (2024); Al-Hawamleh (2023), have explored issues at the ground level but are mainly about technological solutions rather than governance and coordination. This discrepancy calls for a holistic approach to cyber security that addresses both technical elements of cyber security, but also the governance structures and international collaboration for improved security of national websites.

This study is an attempt to examine what cyber risks and threats Pakistani national websites are facing and suggest appropriate governance and international co-operation solutions to mitigate these risks and threats. In this research, we also want to prioritise these measures by ISM-MICMAC (Interpretive Structural Modelling and Matrix of Cross-Impact Multiplications Applied to a Classification). It would use ISM-MICMAC methodology to simulate the relationships between various cyber security actions and rank them according to their importance and impact. It is in this regard that the ISM-MICMAC methodology comes in handy, evaluating direct and indirect associations between measures, and then making recommendations on which interventions are the most important to follow.

This manuscript contributes greatly to cyber security by discussing the unique problems of Pakistani national government websites. It is the first of its kind research that employs the ISM-MICMAC framework to rank and assess cyber security measures about governance and international cooperation. By using this methodology and a Pakistani context, the research presents a complete perspective on cyber security and feasible recommendations for making government websites safer. This research will assist policymakers, cyber security practitioners and global partners in planning to protect Pakistan's vital digital infrastructure from the malicious new threats.

2. Literature Review

2.1. Global cyber security landscape

Cybersecurity is a world-wide issue with increasing and advanced cyber threats. Cybercrime is one of the world's most widespread forms of crime, with a report from the International Telecommunication Union (ITU) projecting a global cybercrime burden of $10.5 trillion a year by 2025 (El-Moghazi & Whalley, 2022). Global nations now implement severe cyber security measures against these attackers and global organizations are ramping up their cybersecurity. In the US, for instance, the Cybersecurity and Infrastructure Security Agency (CISA) has been created to operate and develop US infrastructure security primarily focused on risk management and real-time incident response (Nawaz et al., 2024). The European Union's General Data Protection Regulation (GDPR) has also become a data and privacy standard-setting instrument that will set the world's standards when it comes to online user privacy (Bederna & Rajnai, 2022).

Asia like China and Japan have implemented comprehensive cyber security protocols. China introduced the Cybersecurity Law which requires companies to follow strict data privacy policies, monitor and report cyberattacks and localize data. Implementation of the law is meant to protect national interests and infrastructure. Japan, meanwhile, is more interested in training cybersecurity talent and has integrated cyber defence with its military and public sectors. This has led Japan to

have a significant improvement in cyber resilience and now sits 5th in the world on the Global Cybersecurity Index (GCI). Japan's national Cybersecurity Centre also continuously monitors holes and ramps up public-private partnership to mitigate new threats, especially national initiatives such as the Tokyo Olympics (Noor et al., 2024).

The European Union Agency for Cybersecurity (ENISA) also assists the EU member states with increasing cyber security preparedness. ENISA focuses on unified cyber security risks and challenges for cross-border cooperation. For instance, in 2020 ENISA prepared a Cybersecurity Strategy for the Digital Decade to secure the EU from cyber risks and enable digital transformation. The plan seeks a greater defence of infrastructures critical to the public good, and EU countries such as Estonia are doing most of the work. Estonia – with its e-government and digital society – is already a world leader in cyber security and is using blockchain to protect online services, such as voting, banking and identity (Dunn Cavelty & Smeets, 2023).

Middle Eastern countries have also upped their cyber security in recent years. Saudi Arabia, for example, has an authority in place for cyber security (the Saudi National Cybersecurity Authority, or NCA), which protects the nation's critical infrastructure and critical sectors against cyberattacks. Saudi Arabia's NCA has the leading roles in projects like Cybersecurity Shield to secure critical sectors such as energy and telecommunications. In the same vein, the United Arab Emirates (UAE) has had its own cyber security plan that has focused on establishing national cyber resilience, digital security systems, and public and private sector awareness and training. As a result of this, the UAE is now one of the most technologically advanced nations in the Middle East when it comes to cyber security (Othman et al., 2025).

All these initiatives worldwide call for more holistic, multilayered cyber security approaches – government regulation, private sector collaboration, and innovation. As more advanced threats — ransomware, APTs, and state sponsored attacks — evolve in the world, nations are focusing on cyber security to ensure citizens, economies and national security. The global cyber security response will need to adapt with changes in the cyber threat landscape so governments and companies can effectively mitigate risks and respond to incidents (Bruggemann et al., 2022).

2.2. Challenges and cyber security issues related to Pakistani national websites

Pakistan has also faced severe cyber security issues due to its growing digital network. A 2019 report from the Pakistan Telecommunication Authority (PTA) also pointed out that Pakistan is one of the most popular nations where hackers are increasingly attacking financial institutions, governments and telecom companies. Cybercrimes such as phishing, ransomware, and hacking have also brought to the fore concerns regarding the fragility of infrastructure (Baloch et al., 2022). The absence of solid laws and national cyber security programs have only exacerbated these issues. Although the Pakistan Cyber Security Policy 2021 has been introduced, the execution and enforcement of its rules is still very weak, which makes the country vulnerable to external and internal attacks. Because of increasing use of digital platforms, Pakistan's cyber-security infrastructure needs huge investments and improvements in terms of technology, training and security (Ahmad, 2022).

That's always been a problem with Pakistani government websites as they are a target for hackers and cyber criminals. Numerous major attacks on government websites have exposed weaknesses in the national grid. More than 100 government websites were hacked or breached during a series of cyberattacks in 2020, as Pakistan's Ministry of Information Technology and Telecommunication (MoITT) has reported. And hackers can also hack into a website's content or gain unauthorized

access to data for reputational and commercial damage. The hack of the National Database and Registration Authority (NADRA) in 2017, which exposed the identities of millions of Pakistanis, is the best known. And security efforts aside, ongoing hacking of government websites, such as the Ministry of Defence website in 2021, shows that cyber crime isn't dead and there is no adequate defence (Saleem, 2024).

What's the biggest weakness of Pakistan's cyber-defence system for state-owned websites is that it lacks a centralised, coordinated response to attacks. Agencies typically operate in silos and are not exchanging threat intelligence or best practices. Using this separate method makes sites vulnerable to more sophisticated attacks. Even the Pakistan Telecommunication Authority (PTA) fell victim to a cyber attack in 2020 that exposed the personal information of The European Union Agency for Cybersecurity (ENISA) also assists the EU member states with increasing cyber security preparedness. ENISA focuses on unified cyber security risks and challenges for cross-border cooperation. For instance, in 2020 ENISA prepared a Cybersecurity Strategy for the Digital Decade to secure the EU from cyber risks and enable digital transformation. The plan seeks a greater defence of infrastructures critical to the public good, and EU countries such as Estonia are doing most of the work. Estonia – with its e-government and digital society – is already a world leader in cyber security and is using blockchain to protect online services, such as voting, banking and identity (Dunn Cavelty & Smeets, 2023).

Middle Eastern countries have also upped their cyber security in recent years. Saudi Arabia, for example, has an authority in place for cyber security (the Saudi National Cybersecurity Authority, or NCA), which protects the nation's critical infrastructure and critical sectors against cyberattacks. Saudi Arabia's NCA has the leading roles in projects like Cybersecurity Shield to secure critical sectors such as energy and telecommunications. In the same vein, the United Arab Emirates (UAE) has had its own cyber security plan that has focused on establishing national cyber resilience, digital security systems, and public and private sector awareness and training. As a result of this, the UAE is now one of the most technologically advanced nations in the Middle East when it comes to cyber security (Othman et al., 2025).

All these initiatives worldwide call for more holistic, multilayered cyber security approaches – government regulation, private sector collaboration, and innovation. As more advanced threats — ransomware, APTs, and state sponsored attacks — evolve in the world, nations are focusing on cyber security to ensure citizens, economies and national security. The global cyber security response will need to adapt with changes in the cyber threat landscape so governments and companies can effectively mitigate risks and respond to incidents (Bruggemann et al., 2022).

2.3. Challenges and cyber security issues related to Pakistani national websites

Pakistan has also faced severe cyber security issues due to its growing digital network. A 2019 report from the Pakistan Telecommunication Authority (PTA) also pointed out that Pakistan is one of the most popular nations where hackers are increasingly attacking financial institutions, governments and telecom companies. Cybercrimes such as phishing, ransomware, and hacking have also brought to the fore concerns regarding the fragility of infrastructure (Baloch et al., 2022). The absence of solid laws and national cyber security programs have only exacerbated these issues. Although the Pakistan Cyber Security Policy 2021 has been introduced, the execution and enforcement of its rules is still very weak, which makes the country vulnerable to external and internal attacks. Because of increasing use of digital platforms, Pakistan's cyber-security infrastructure needs huge investments

and improvements in terms of technology, training and security (Ahmad, 2022).

That's always been a problem with Pakistani government websites as they are a target for hackers and cyber criminals. Numerous major attacks on government websites have exposed weaknesses in the national grid. More than 100 government websites were hacked or breached during a series of cyberattacks in 2020, as Pakistan's Ministry of Information Technology and Telecommunication (MoITT) has reported. And hackers can also hack into a website's content or gain unauthorized access to data for reputational and commercial damage. The hack of the National Database and Registration Authority (NADRA) in 2017, which exposed the identities of millions of Pakistanis, is the best known. And security efforts aside, ongoing hacking of government websites, such as the Ministry of Defence website in 2021, shows that cyber crime isn't dead and there is no adequate defence (Saleem, 2024).

What's the biggest weakness of Pakistan's cyber-defence system for state-owned websites is that it lacks a centralised, coordinated response to attacks. Agencies typically operate in silos and are not exchanging threat intelligence or best practices. Using this separate method makes sites vulnerable to more sophisticated attacks. Even the Pakistan Telecommunication Authority (PTA) fell victim to a cyber attack in 2020 that exposed the personal information of thousands of customers. And governmental websites are still using outdated software and hardware, so it is easy to attack by hackers (Dhirani, 2024). Even though basic technologies have been invented, such as firewalls and encryption, other technologies, such as intrusion detection systems (IDS), multi-factor authentication, and regular security audits, aren't good enough in most businesses. Pakistan should solve all these issues with the help of complete cyber security policy, public private partnership and timely review of government's web site security (Saleem, 2025).

2.4. Key cyber security measures

2.4.1. Cyber Security Governance Framework

The national websites security can only be properly governed through a solid cyber security governance framework. Research by the European Union Agency for Cybersecurity (ENISA) in 2020 states that governments effectively countering cyber attacks have clear governance. Through good governance, roles and duties, and the decision process can be defined clearly, which would ensure accountability and govern cyber security more effectively. Hence, for Pakistan's national websites, appropriate cyber security governance framework assists in centralised security, better management of security, security policy aligned to national agenda, risk mitigation and enhanced response (Melaku, 2023).

2.4.2. Compliance with International Standards and Regulations

If the national website complies with international cyber security regulations and legislation, it can be best in class and safe globally. The standards of information security and data privacy are ISO/IEC 27001 and the General Data Protection Regulation (GDPR) which are some of the international standards for information security and data privacy. As the ISO research further indicates, by following these guidelines you can limit vulnerability and protect data. In case of Pakistan, the international standards like GDPR regarding data privacy and ISO 27001 in the information security management will ensure that government websites are safer, and the citizens are more trusting. These frameworks also put Pakistan on international cyber security levels for easier exchange of foreign money and data (Srinivas, 2019).

2.4.3. Centralized Cyber Security Strategy

It's all in a central cyber security solution to maintain consistent and robust policy across government entities and government agencies. The World Economic Forum (WEF) published a report in 2019 calling for the development of a common national cyber security strategy, especially in decentralized economies. Pakistan can avail the benefits of centralized cyber security wherein multiple government agencies can pool security measures and coordinate the response. Then the security holes will be minimized, and all government websites are protected by the same mechanisms, minimizing the possibility of a cyberattack (Jaber, 2025).

2.4.4. Cyber Security Risk Management

Cyber security risk management is the process of reviewing, discovering, and controlling risks related to government websites. Gartner has shown that states with robust risk management are better prepared to recognize new threats and take steps to address them. For Pakistan, a risk management model would help prioritise resources and efforts to safeguard the most valuable government websites. In identifying the impacts of different cyber threats and vulnerabilities, Pakistani government can create custom-built mitigation plans so that the critical systems are sufficiently protected while maximizing the utilization of resources (Mızrak, 2023).

2.4.5. National Cyber Security Strategy and Policy

National cyber security strategy is the guide for national infrastructure and government websites security. The Global Forum on Cybersecurity Policy (2019) noted that countries need to adopt national policies with clear goals, steps, and funding to tackle cyber-attacks. In Pakistan, a global cyber security policy and local cyber threat, which will enable a coordinated response against cyber attacks on government websites, would also serve as a national cyber security policy. It also has to include a periodic monitoring and upgrading process so it can keep up with the evolving threat landscape (Bechara, 2021).

2.4.6. Cyber Security Awareness and Capacity Building

Increasing public awareness and ability among government organizations is critical to a secure cyber security governance. Training and capacity-building will allow public servants to recognise and address cyber attacks, a United Nations report on digital governance in 2020 stated. For government websites of Pakistan, continuing training on best practices for cyber security will be done to equip employees with information and expertise to manage cyber risks. What's more, raising awareness about cyber security among the masses will create a spirit of online security and precaution which will minimize the likelihood of attacks on national websites (Collett, 2021).

2.4.7. Public-Private Collaboration for Cyber Defence

Public and private sector cooperation is the answer to tackling complex cyber security problems. Public-private partnerships promote greater access to threat intelligence and resources, increasing cyber defences, according to a 2018 report from the Cybersecurity & Infrastructure Security Agency (CISA). For Pakistan, bringing together the government, private tech companies, and universities will enhance the cyber security of national websites. Sharing real time threat information and engaging private sector cyber defence experts can make Pakistan a better cyber security system (Haklai, 2023).

2.4.8. International Cyber Security Cooperation

Global cyber-attacks need global partnership to mitigate and respond. Research by the International Telecommunication Union (ITU) indicates that global cyber cooperation in combating cross-border attacks (ransomware, cyber-espionage) is key. Pakistan should also beef up relations with

international agencies like UN and INTERPOL for the sharing of threat intelligence, co-operation in cyber defences and cyber incident response in real time. Pakistan can help protect government websites and help global battle against cybercrime by participating in international cyber security programs (Naseeb, 2024).

2.4.9. Cyber Security Framework for Government Websites

A dedicated cyber security framework to government websites can enhance security and conformity to the national guidelines. As a Deloitte report (2020) pointed out, custom security infrastructure for government entities mitigates risk and makes security administration simple. Such a framework, in the case of Pakistan, would define protocols to protect national websites, standardize security procedures and help the government agencies adhere to law and regulations. It would also allow for federation of state entities in the interest of digital infrastructure security.

2.4.10. Incident Reporting and Response Coordination

Cyber Incident Reporting and Response between government agencies is essential to reducing impact of cyber attack. A McKinsey report in 2019 shows that the faster organisations react to attacks, the better they can protect themselves. Similarly, Pakistan can take cyber security governance a step further and establish a national cyber incident response centre (CIRC) for centralized reporting, investigation and management of cyber incidents against the state websites. This would allow attacks to be stopped sooner, damage limited, and hackers prosecuted accordingly (Busetti, 2025).

2.4.11. Secure Software Development Lifecycle (SDLC)

Security Secure Software Development Lifecycle (SDLC) allows you to apply security across the entire development lifecycle. In OWASP research, it was found that SDLC practices minimize vulnerabilities and increase web application security. For Pakistan, ensuring all government websites and web services get comprehensive security testing during the development process will help keep common security risks like SQL Injection or Cross-Site Scripting (XSS) at bay. Secure coding practices and code reviews can lead to early discovery and elimination of vulnerabilities before they can be deployed (McCoy, 2025).

2.4.12. Cyber Crisis Management and Contingency Planning

Cyber crisis management helps governments act quickly in case of a large cyber event, so that services are disrupted as little as possible and back up and running. A 2019 report from the National Cyber Security Centre (NCSC) recommended preparing an elaborate emergency response to cyber attacks. If Pakistan created a dedicated cyber crisis management team for each government department, cyberattacks on national websites could be addressed quickly. They need to be trained on-the-job, so they are equipped for any type of cyber attack, such as a data breach, DDoS attack, or malware infection, and capable of a fast and unified recovery (Bıçakcı, 2024).

2.4.13. Cyber Security Auditing and Accountability

Periodic cyber security audits allow you to spot weaknesses and comply with security policies. ISACA research (2020) concludes that auditing can greatly contribute to improving security postures and holding government entities accountable for cybersecurity. The implementation of periodic third-party audits by independent third parties for Pakistan's nation website would ensure that the security measures are kept current and efficient. Auditing also helps identify weaknesses and make recommendations for improving security at government sites (Slapničar et al., 2023).

2.4.14. Cyber Security Threat Intelligence Sharing Networks

Establishing national and international threat intelligence sharing systems increase cyber threat detection and response. As The World Economic Forum (2019) discovered, when threat intelligence is shared, businesses can better predict and protect themselves from new cyber threats. In the case of Pakistan, setting up a cyber security threat intelligence sharing network will allow government agencies to exchange information on current threats and vulnerabilities. Also, working with overseas entities will make Pakistan better able to thwart global attacks by protecting national websites from sophisticated attacks (Goni, 2022).

2.4.15. International Cyber Security Legal Frameworks and Compliance

Keeping national cyber security efforts in line with global laws can support global cooperation and strengthen cybersecurity. As UNODC (2020) suggests, linking national cyber security policies to international agreements like the Budapest Convention on Cybercrime enables international legal collaboration to combat cyber-attacks. Pakistan should secure its government websites and join international cyber security treaties and conventions, which would also provide an open border for cyber-crime fighting, sensitive data security, and digital infrastructure resilience at the national level (Ali, 2024).

2.5. Application of ISM-MICMAC approach to analyse cyber security measures

The ISM and MICMAC (Matrix of Cross-Impact Multiplications Applied to a Classification) models are increasingly being used in cyber security research to construct deep relationships and discover the most important security determinants. This can be used to structure large-scale systems because it determines the direct and indirect relationships between various variables, and it shows us clearly how various metrics impact on each other. According to Etemadi et al. (2021) ISM-MICMAC helps cybersecurity researchers to determine priority steps, discover their relationships and classify them based on relative importance and impact. This is particularly helpful when more than one factor (e.g., organizational processes, technology and government structures) needs to be considered simultaneously. Creating an architectural description of what constitutes a cyber security architecture and how those parts relate to each other helps determine the best cybersecurity defences.

ISM-MICMAC can be used specifically when ranking cyber security solutions, since it provides a method to determine how security solutions are interrelated and driving one another (Hussain et al., 2024). Regarding Cyber Security of Pakistani National Websites, ISM-MICMAC can be utilized to identify correlations between various cyber security elements (Data encryption, multi-factor authentication, incident response mechanisms, employee training etc.) Analysing how these measures interrelate with each other, the methodology makes sense of which measures are most crucial for overall security, and which rely on others to work. This is especially beneficial in Pakistan, where resources are limited, and efficient security solutions require that the best measures for the security of the national websites should be implemented (Hussain et al., 2023).

For Pakistan, the ISM-MICMAC ranking of cyber security precautions for government websites is especially suited considering the nature of the cyber threat that government websites face is dynamic and changing. Pakistan's cyber security is also dependent on many variables such as technology infrastructure, policy, human resources, and global collaboration. Researchers and policymakers can use the ISM-MICMAC methodology to find the most effective security measures and determine their viability. For instance, compliance with international standards, improved governance systems, and increased public-private cooperation could all be perceived as driving security overall (Asif et

al., 2025). Furthermore, ISM-MICMAC approach can also highlight interdependencies among such measures to define a holistic approach for solving Pakistan's unique cyber security issue. It is through this method that Pakistan can better spend its resources and construct a comprehensive and effective stratified defence system.

3. Research Methodology

This paper uses a multi-phase systematic approach based on systems thinking and analytical modeling to understand the relationships between cybersecurity of national websites of the government. The method is created in a way that it reveals the structural dependencies and gives priorities to interventions using a mix of both expert elicitation and formal modeling methods (Naheed et al., 2024). The research approach will be made up of four consecutive stages (as shown in Figure 1) as follows:

Step 1. Identification of Cybersecurity Measures

The initial step was the systematic search of the possible cybersecurity measures that could be applicable to the security of national digital infrastructure. The exhaustive analysis of scholarly literature, global standards and policy documents was done to list an initial list of candidate measures (Iqbal et al., 2025). This move guaranteed the wide scope of technical, organizational, and strategic aspects of cybersecurity governance. A final list of measures is shown in Table 1.

Table 1. List of Cybersecurity measures

Code	Measure
M1	Cyber Security Governance Framework
M2	National Cyber Security Strategy and Policy
M3	Cyber Security Risk Management
M4	Cyber Security Awareness and Capacity Building
M5	Public-Private Collaboration for Cyber Defence
M6	International Cyber Security Cooperation
M7	Cyber Security Threat Intelligence Sharing Networks
M8	Incident Reporting and Response Coordination
M9	Secure Software Development Lifecycle (SDLC)
M10	Cyber Crisis Management and Contingency Planning
M11	Cyber Security Auditing and Accountability
M12	Centralized Cyber Security Strategy

Step 2. Filter measures using Fuzzy Delphi Method (FDM)

The Fuzzy Delphi Method (FDM) was used to filter the original list and reach an agreement on the relevance of each of the measures. An expert panel was established to review the measures through linguistic scales in an organized and iterative consultation. The approach facilitated the minimization of uncertainty and harmonization of the views of the experts with the help of recurrent feedback and only the measures that receive high consensus were left to be analyzed further. In total three measures were deleted through this method and the final file after filtering is found in Table 1.

Step 3: Interpretive Structural Modeling (ISM)

Interpretive Structural Modeling (ISM) was applied to show the hierarchical relationships between cybersecrity measures. There is a Structural Self-Interaction Matrix (SSIM) that was built on expert estimates to represent directional effects among pairs of measures. This matrix was in turn transformed into an Initial Reachability Matrix (IRM) which was followed by the transitivity analysis to obtain Final Reachability Matrix (FRM). In level partitioning, the measurements were structured into a hierarchical form of level and allowed the visualization of the underlying drivers and dependent outcomes in the format of directed digraph.

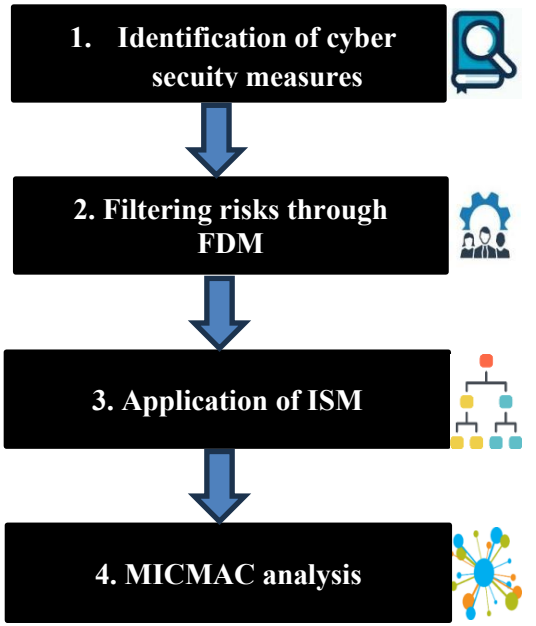

Figure 1Step by step study approach

Step 4: Classification through MICMAC Analysis

The hierarchical form based on ISM was further to be examined by MICMAC (Matrice d'Impacts Croisages Multiplication Appliquage a un Classement) method. This approach treats each measure as the driving power (how much it affects other measures) and dependence power (how much it is affected by other measures). The resulting classification positions measures in four quadrants, namely Independent, Dependent, Linkage, and Autonomous, that give a framework of how they fit in their strategic roles in the larger cybersecurity infrastructure.

3.1. Application of ISM-MICMAC methodology

SSIM development:

At the first step, a Structural Self-Interaction Matrix based on pair-wise comparison of the chosen elements was established. Directional relationships may be indicated by use of symbols (V, A, X, O) where symbol shows the following:

V: Element i influences j

A: Element j influences i
X: Element j and i influence each other
O: No relationship

Table 2. SSIM

Measures	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
M1	–	V	V	V	V	V	V	V	V	V	V	V
M2	A	–	V	V	V	V	V	V	V	V	V	X
M3	A	A	–	V	V	A	V	V	V	V	V	V
M4	A	A	A	–	V	A	V	A	V	A	V	A
M5	A	A	A	A	–	X	X	A	A	A	A	A
M6	A	A	V	V	X	–	X	A	A	A	A	A
M7	A	A	A	A	X	X	–	A	A	A	A	A
M8	A	A	A	V	V	V	V	–	A	X	V	A
M9	A	A	A	A	V	V	V	V	–	V	V	A
M10	A	A	A	V	V	V	V	X	A	–	V	A
M11	A	A	A	A	V	V	V	A	A	A	–	A
M12	A	X	A	V	V	V	V	V	V	V	V	–

Transform SSIM into IRM:
Turn the SSIM into a binary Initial Reachability Matrix, using symbols in place of 1s (influence) and 0s (no influence), and by processing the directional logic of V, A, X, O. (Table 3)

Use Transitivity:
Test on transitivity (i → j and j → k) and make appropriate changes on the IRM to constitute the Final Reachability Matrix (FRM). Results for FRM are shown in Table 4.

Identify Reachability and Antecedent Sets:
Reachability set: The elements that it can affect (including itself) *Antecedent set:* It is all the elements which can affect it (including itself).

Table 3. IRM

Measures	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
M1	1	1	1	1	1	1	1	1	1	1	1	1
M2	1	1	1	1	1	1	1	1	1	1	1	1
M3	0	0	1	1	1	0	1	1	1	1	1	1
M4	0	0	0	1	1	0	1	0	1	0	1	0
M5	0	0	0	0	1	1	1	0	0	0	0	0
M6	0	0	1	1	1	1	1	0	0	0	0	0

M7	0	0	0	0	1	1	1	0	0	0	0	0
M8	0	0	0	1	1	1	1	1	0	1	1	0
M9	0	0	0	0	1	1	1	1	1	1	1	0
M10	0	0	0	1	1	1	1	1	0	1	1	0
M11	0	0	0	0	1	1	1	0	0	0	1	0
M12	1	1	1	1	1	1	1	1	1	1	1	1

Table 4. FRM

Measures	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
M1	1	1	1	1	1	1	1	1	1	1	1	1
M2	1	1	1	1	1	1	1	1	1	1	1	1
M3	0	0	1	1	1	1	1	1	1	1	1	1
M4	0	0	0	1	1	1	1	1	1	1	1	0
M5	0	0	0	0	1	1	1	1	1	1	1	0
M6	0	0	0	0	1	1	1	1	1	1	1	0
M7	0	0	0	0	1	1	1	1	1	1	1	0
M8	0	0	0	0	0	0	0	1	0	1	1	0
M9	0	0	0	0	0	0	0	1	1	1	1	0
M10	0	0	0	0	0	0	0	1	0	1	1	0
M11	0	0	0	0	0	0	0	0	0	0	1	0
M12	1	1	1	1	1	1	1	1	1	1	1	1

Level Partitioning:

The intersection of reachability and antecedent sets are equal to the reachability set. They are the ones that are positioned at the highest level (e.g., Level I). Wipe out and reiterate until you have left only a few elements which are then placed at subsequent lower levels (Level II, III, etc.). Results for all rounds of levels partition are given in below given tables (Table 5 to Table 7)

Table 5. Level Partition (1)

Mi	R(Mi)	A(Mi)	I(Mi)	Level
M1	All	M1,M2,M12	M1,M2,M12	No
M2	All	M1,M2,M12	M1,M2,M12	No
M3	M3–M12	M1,M2,M3,M12	M3,M12	No
M4	M4–M11	M1,M2,M3,M4,M12	M4	Yes → Level IV

M5	M5–M11	M1–M7,M9,M10,M12	M5	Yes → Level IV
M6	M5–M11	M1–M7,M9,M10,M12	M6	Yes → Level IV
M7	M5–M11	M1–M7,M9,M10,M12	M7	Yes → Level IV
M8	M8,M10,M11	M1–M10,M12	M8,M10	No
M9	M8–M11	M1–M5,M7,M9,M12	M9	Yes → Level III
M10	M8,M10,M11	M1–M10,M12	M8,M10	No
M11	M11	M1–M11,M12	M11	Yes → Level II
M12	All	M1,M2,M12	M1,M2,M12	No

Table 6. Level Partition (2)

Mi	R(Mi)	A(Mi)	I(Mi)	Level
M1	M1,M2,M3,M8,M9,M10, M11,M12	M1,M2,M12	M1,M2,M12	No
M2	same	M1,M2,M12	M1,M2,M12	No
M3	M3,M8,M9,M10,M11,M12	M1,M2,M3,M12	M3,M12	No
M8	M8,M10,M11	M1–M3,M8,M9,M10,M12	M8,M10	No
M9	M8,M9,M10,M11	M1–M3,M9,M12	M9	Yes → Level III
M10	M8,M10,M11	M1–M3,M8,M9,M10,M12	M8,M10	No
M11	M11	M1–M3,M8–M11,M12	M11	Already Level II
M12	all	M1,M2,M12	M1,M2,M12	No

Table 7. Level Partition (3)

Mi	R(Mi)	A(Mi)	I(Mi)	Level
M8	M8,M10,M11	M1–M3,M8,M10,M12	M8,M10	No
M10	M8,M10,M11	M1–M3,M8,M10,M12	M8,M10	No
M11	M11	...	M11	Level II (confirmed)

Build the ISM Digraph:

Build a hierarchical model (digraph) in terms of the level partitions, indicating directional

relationships between elements at levels. Final ISM diagraph is shown in Figure 2.

Developing ISM model:
Finally, a final ISM model is established based on the diagraph and description of each element is placed in the hierarchal model (diagraph). Final ISM model is shown in Figure 3.

MICMAC Analysis:
Arrange elements in four groups in terms of their driving power (capability to impact others) and dependence (degree to which they are impacted); Autonomous, Dependent, Linkage Independent (Key Drivers). Results for MICMAC analysis are shown further in Figure 4.

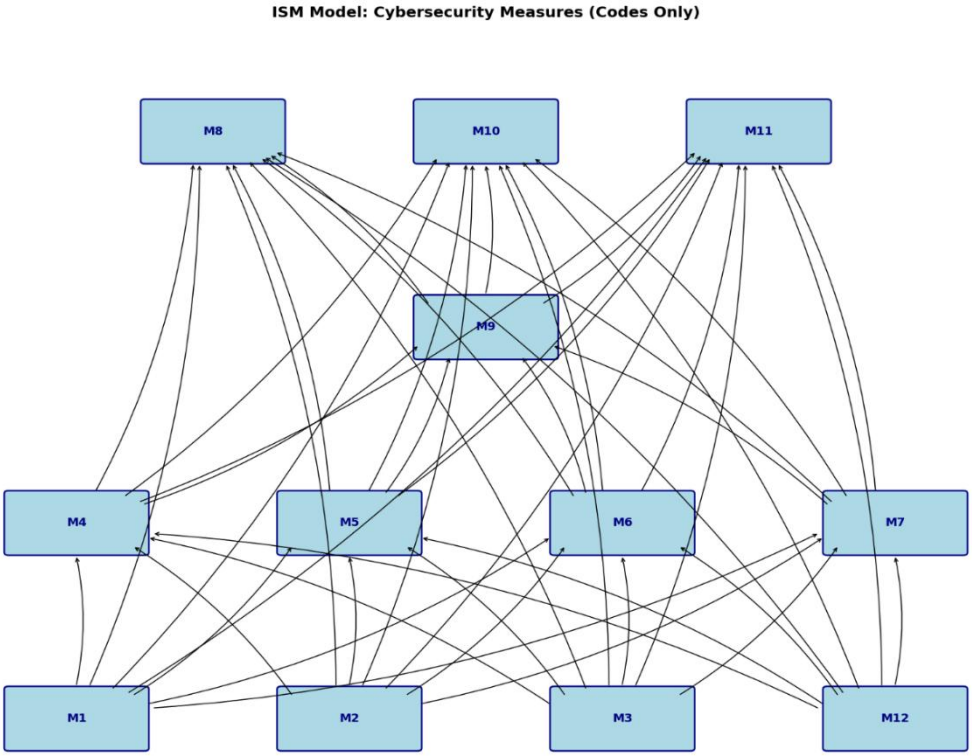

Figure 2Final Diagraph for the study

4. Results and discussion

An analysis using the Interpretive Structural Modeling (ISM) shows that cybersecurity measures toward national websites in Pakistan are well hierarchically structured with four root driver variables serving as the bottom tier (Level IV) which are Cyber Security Governance Framework (M1),

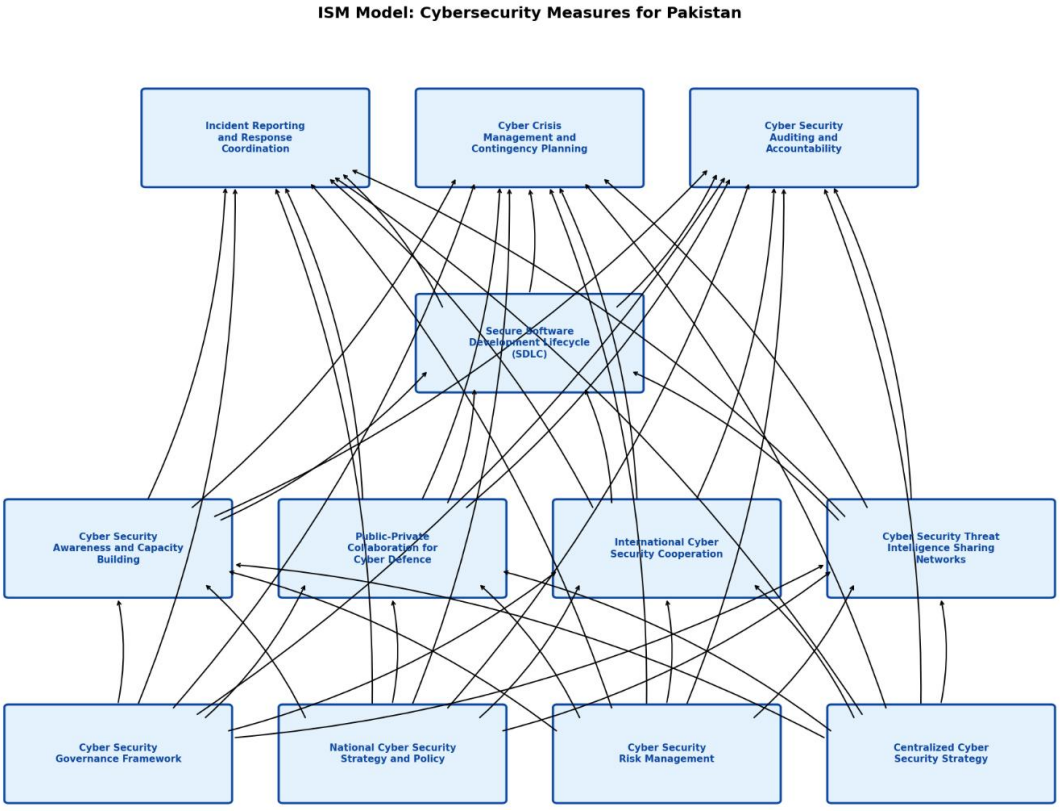

Figure 3 Final ISM model for the study

National Cyber Security Strategy and Policy (M2), Cyber Security Risk Management (M3), and Centralized Cyber Security Strategy (M12). These measures have the greatest driving power and begin at M1.

Intimately connected to governance is the National Cyber Security Strategy and Policy (M2) that gives the vision, goals, and plan of cybersecurity implementation. Pakistan has long been functioning with no officially approved and publicly accessible national cybersecurity strategy and instead having to rely on informal directives and draft frameworks that do not have legal authority or budgetary support. ISM hierarchy makes M2 and M1 on the same level of foundations since a strategy without governance has no one to enforce its strategies and governance without strategies has no direction to follow. Lacking a binding national policy has created unequal security postures in the different ministries, where only three of the eighteen federal entities currently have formal cybersecurity guidelines (as at 2025). An all inclusive, legislated National Cyber Security Strategy 20252030, that is in line with the Digital Pakistan Vision and the international best practices would

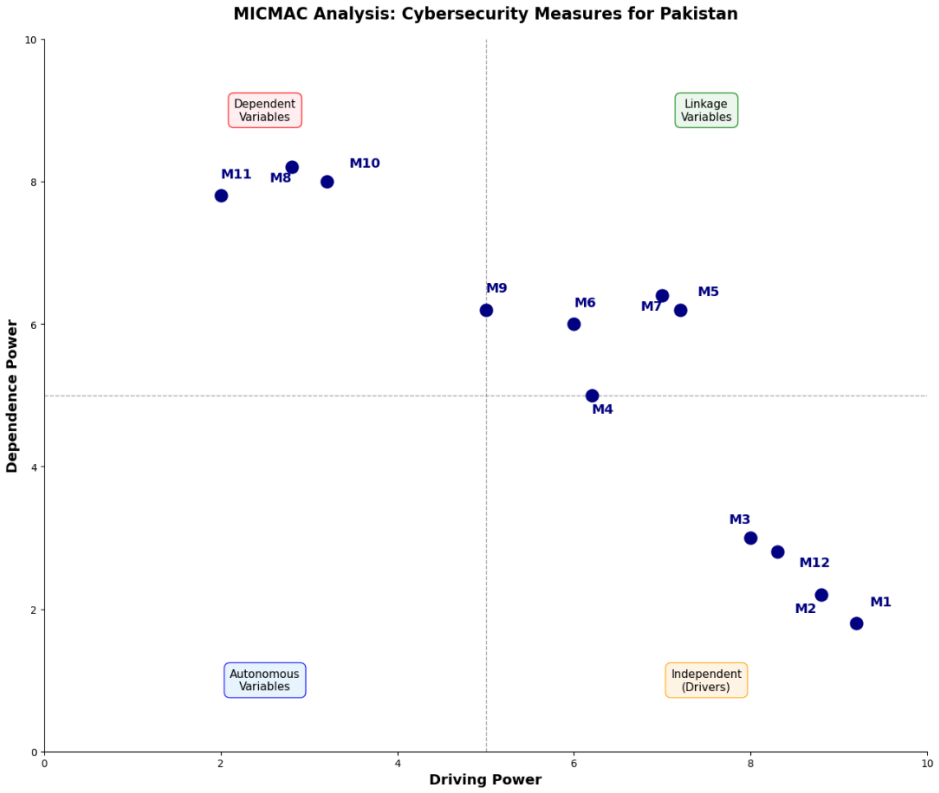

Figure 4 MICMAC analysis

help clarify roles, allocate resources, and set schedules in which the strategy is executed. Most importantly, it would show domestic dedication to the national stakeholders and the international partners and increase trust and allow cooperation. The ISM model can prove that M2 is not just a document, it is a requirement to the coherence of the whole cybersecurity ecosystem.

The third element of the bottom layer is Cyber Security Risk Management (M3), which reflects the strategic intent into operational reality. Risk management has remained event-driven, reactive, and informal in Pakistan with no standardized approach to identifying, assessing, and minimizing cyber threats in the government systems. The ISM analysis makes M3 a root driver since good risk management will allow prioritization to be made whereby limited resources will be focused on safeguarding the most important assets. In the absence of an established risk management model based on a standard like ISO/IEC 27005 or NIST SP 800-30, the agencies would not be able to assess vulnerabilities systematically, measure possible impacts, and rationalize security expenditures. This creates a kind of whack-a-mole tactic in which answers are provided by the most recent newsworthy assault and not a level-headed evaluation of systemic exposure. Making risk management an obligatory process in all federal ministries, beginning with the 50 most significant national websites, would change the attitude of Pakistan towards reactive mode of security

operations to proactive mode, such that the safety operations are not only focused but effective as well.

M12 Centralized Cyber Security Strategy is the fourth founding measure which handles the operational aspect of action and coordination. As M1 stipulates institutional authority and M2 gives strategic direction, M12 makes sure that these are converted to a single operational front. The decentralized nature of cybersecurity in Pakistan, with the various ministries or agencies taking charge of their defense, poses a dangerous blind spot and inefficiencies. M12 envisages a Federal Cyber Command Center (FCCC) that would act as the nerve center of real-time monitoring and threat detection as well as coordinated response of all the government entities. It would remove redundancy and facilitate mutual situational awareness and make sure that failure in any agency does not spill over to others because of insufficient time to warn them. The ISM model underscores the driving force of M12 since centralization increases the efficiency of all other interventions: it renders governance enforceable, the strategy implementable, the risk management scaleable. Basically, M12 is the connective tissue that adheses the base layer into a functional unit.

One of the important lessons of the ISM analysis is that all these four root drivers are interdependent. They are not independent of each other but in a virtuous circle, support each other. Good governance (M1) can give rise to the implementation and execution of a national strategy (M2); a definite strategy will give the mandate to systematic risk management (M3); risk-informed decisions will be the justification of investing in centralized coordination (M12); and which in turn will reinforce governance by way of increased oversight. This is a cyclic reinforcement, where the half-baked measures like applying a strategy that is not governed or centralizing operations without risk analysis will give sub Apoptic outcomes. The way ahead of Pakistan should thus be comprehensive: these four things should be promoted simultaneously, with their complementation, and not in the strict sequence. The upper-level measures, including incident response, auditing, or the collaboration of the entities, are also meaningful results, although the hierarchy of the ISM makes it absolutely clear that they are dependent variables. They do not deserve to be successful but solely on how strong their foundation is. Therefore, the prioritization of policy and resources should be placed on M1, M2, M3, and M12, not as the initial phase, but the sustainable center of the Pakistan cybersecurity infrastructure.

5. Conclusion

In conclusion, the paper has shown that the national sites of Pakistan must be secured not only as a technical issue, but as a governance necessity as well. The ISM-MICMAC analysis is categorical in demonstrating that achieving sustainable cybersecurity is beyond patching system vulnerabilities or responding to incidents in vacuums. Rather, it involves a conscious, top-down reorganisation of institutional structures, which starts with the introduction of evident governance, a consistent national strategy, and institutionalised risk management procedures. It is these ground-breaking building blocks that give life to all other actions that include teamwork, sharing of intelligence, development in safety, and response. In their absence, the cybersecurity effort will be partially disjointed, reactive, and ultimately ineffective. The gradual implementation plan presented here will provide a viable, low cost, approach to help Pakistan change its cyber posture within three years, using existing institutions but developing new capabilities where needed. The first important step is driver variables, as a result of which the nation will be able to create a self-reinforcing ecosystem where each next layer of security is stronger and more significant. The necessity of the change is

hard to overestimate in the age when the concept of digital infrastructure is defined as national sovereignty, they leave the doors of the state open by not protecting government websites. It is in the interest of Pakistan to shift its position of vulnerability into that of strength. The blueprint is there, the only thing that is required is political determination, strategic investment as well as institutional dedication to actualize this vision. This policy review should not be an exercise in theory, but a call to action to policymakers, technologists, and citizens in Pakistan to protect the digital future in this country.

References:

Ahmad, S. (2022). Cyber security threat and Pakistan's preparedness: An analysis of national cyber security policy 2021. *Pakistan Journal of Humanities & Social Sciences Research, 5*(1), 33.

Ajiga, D., Okeleke, P. A., Folorunsho, S. O., & Ezeigweneme, C. (2024). Designing cybersecurity measures for enterprise software applications to protect data integrity. *Computer Science & IT Research Journal, 5*(8), 1920-1941.

Al-Hawamleh, A. M. (2023). Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures. *momentum, 3*, 15.

Ali, M. (2024). Cybercrime and Cybersecurity: A Critical Analysis of Legal Frameworks and Enforcement Mechanisms. *Bharati International Journal of Multidisciplinary Research and Development, 2*(8), 137-154.

Asif, M., Shah, H., & Asim, H. A. H. (2025). Cybersecurity and audit resilience in digital finance: Global insights and the Pakistani context. *Journal of Asian Development Studies, 14*(3), 560-573.

Baloch, U., Muhammad, B., & Niaz, T. (2022). Pakistan's Cyber Security Governance: Challenges and Way Forward. *Insight*.

Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and global regulatory challenges. *Journal of Financial Crime, 28*(2), 359-374.

Bederna, Z., & Rajnai, Z. (2022). Analysis of the cybersecurity ecosystem in the European Union. *International Cybersecurity Law Review, 3*(1), 35-49.

Bıçakcı, S., & Evren, A. G. (2024). Responding cyber-attacks and managing cyber security crises in critical infrastructures: A sociotechnical perspective. In *Management and Engineering of Critical Infrastructures* (pp. 125-151): Elsevier.

Bruggemann, R., Koppatz, P., Scholl, M., & Schuktomow, R. (2022). Global cybersecurity index (GCI) and the role of its 5 pillars. *Social Indicators Research, 159*(1), 125-143.

Busetti, S., & Scanni, F. M. (2025). Evaluating incident reporting in cybersecurity. From threat detection to policy learning. *Government Information Quarterly, 42*(1), 102000.

Collett, R. (2021). Understanding cybersecurity capacity building and its relationship to norms and confidence building measures. *Journal of Cyber Policy, 6*(3), 298-317.

Dhirani, L. L. (2024). *Data Security, Privacy and Cyber Policy of Pakistan: A Closer Look.* Paper presented at the 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC).

Dunn Cavelty, M., & Smeets, M. (2023). Regulatory cybersecurity governance in the making: The formation of ENISA and its struggle for epistemic authority. *Journal of European Public Policy, 30*(7), 1330-1352.

Dutta, N., Jadav, N., Tanwar, S., Sarma, H. K. D., & Pricop, E. (2022). *Cyber security: issues and*

current trends: Springer.
El-Moghazi, M., & Whalley, J. (2022). The itu imt-2020 standardization: Lessons from 5g and future perspectives for 6g. *Journal of Information Policy, 12*, 281-320.
Etemadi, N., Strozzi, F., Van Gelder, P., & Etemadi, T. (2021). *An ISM modelling of success factors for blockchain adoption in a cyber secure supply chain.* Paper presented at the Proceedings of the 2021 4th International Conference on Computers in Management and Business.
Goni, O. (2022). Cyber crime and its classification. *Int. J. of Electronics Engineering and Applications, 10*(1), 17.
Haklai, B. (2023). Cybersecurity private-public partnerships: a bridge to advance global Cybersecurity. *Tex. Tech L. Rev., 56*, 627.
Hussain, K., He, Z., Ahmad, N., Iqbal, M., & Saeed, M. Z. (2023). Establishing a Green, Lean and Six Sigma implementation model for sustainable construction industry: An analysis of driving forces through ISM-MICMAC approach. *Environmental Science and Pollution Research, 30*(11), 30462-30492.
Hussain, K., Sun, H., Ahmad, N., & Iqbal, M. (2024). Assessment of risk factors to Green, Lean, Six Sigma adoption in construction sector: Integrated ISM-MICMAC approach. *Heliyon, 10*(12).
Iqbal, M., Lin, Z., Ahmed, R. I., Ahmad, N., & Hussain, K. (2025). Exploring the paths to big data analytics implementation success in construction projects: an integrated approach. *Engineering, Construction and Architectural Management*.
Jaber, A. (2025). Cybersecurity governance and political structures: Comparing centralized and decentralized approaches to cyber defense. *Comparative Strategy*, 1-20.
Jawhar, S., Miller, J., & Bitar, Z. (2024). *AI-based cybersecurity policies and procedures.* Paper presented at the 2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC).
McCoy, E. (2025). Cybersecurity Real-World Applications for the Software Development Life Cycle. *Land Forces Academy Review, 30*(1), 148-161.
Melaku, H. M. (2023). A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy, 3*(3), 327-350.
Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Research Journal of Business and Management, 10*(3), 98-108.
Naheed, R., Waqas, M., Ahmad, N., Iqbal, M., & Ismail, M. (2024). Fostering sustainability and green innovation reporting in manufacturing firms: an investigation of barriers through ISM-MICMAC approach. *Environment, Development and Sustainability*, 1-43.
Naseeb, S., & Khan, W. N. (2024). Mitigating cybercrime through international law: the role of global cybersecurity agreements. *Mayo Communication Journal, 1*(1), 31-40.
Nawaz, H., Sethi, M. S., Nazir, S. S., & Jamil, U. (2024). Enhancing national cybersecurity and operational efficiency through legacy IT modernization and cloud migration: A US perspective. *Journal of Computing & Biomedical Informatics, 7*(02).
Noor, H., Seelro, D. K., & Ali, S. A. (2024). *Review of national cybersecurity policies: a case study on Asian countries.* Paper presented at the 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC).
Othman, S. N., Jawad, A. M., Hameed, R., Kawad, R. T., & Khlaponin, D. (2025). The impact of cybersecurity law in the middle east. *Encuentros: Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico*(23), 392-420.

Saleem, B., Ahmed, M., Zahra, M., Hassan, F., Iqbal, M. A., & Muhammad, Z. (2024). A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap. *International Cybersecurity Law Review, 5*(4), 533-561.

Saleem, H. A. R., Bukhtiar, A., Zaheer, B., & Farooq, M. A. U. (2025). Challenges faced by the judiciary in implementing cybersecurity laws in Pakistan. *The Critical Review of Social Sciences Studies, 3*(1), 1052-1066.

Slapničar, S., Axelsen, M., Bongiovanni, I., & Stockdale, D. (2023). A pathway model to five lines of accountability in cybersecurity governance. *International journal of accounting information systems, 51*, 100642.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future generation computer systems, 92*, 178-188.

Watto, O. M., Islam, M., Hussain, S. A., & Shahab, M. (2024). Cyber law and cyber security policies in pakistan: a comparative study with USA, canada and australia. *Pakistan J Humanit Soc Sci, 12*(1), 271-277.