Data Security, Privacy and Cyber Policy of Pakistan: A Closer Look

Lubna Luxmi Dhirani
Department of Electronic and Computer Engineering
University of Limerick
Limerick, Ireland
lubna.luxmi@ul.ie

2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC) | 979-8-3503-7304-2/24/$31.00 ©2024 IEEE | DOI: 10.1109/KHI-HTC60760.2024.10482125

***Abstract*—Living in an immersive, agile and a fully digital world where the scope, nature and ways of communication, connectivity, operations, business, finance, supply-chain, etc. have all changed and exposed the digital infrastructures and economies to a wider cyber threat landscape. Pakistan, being a developing nation, holds an impressive ranking at the global innovation index 2023, however with these advancements there have been increased security issues and cyber crimes affecting the unprivileged population of the Country. As per the United Nations Sustainable Development Goals 10 and 16, a strong emphasis to reduce inequalities and maintain peace, justice and strong institutions has been given. Unresolving problems affecting the under privileged may contribute to increased hate crime, bias, inequalities, conflicts and prejudice. This paper sheds light on the pressing issues related to lack of data and information security controls enabling misuse of personal identifiable information (i.e., name, health data, geotags, etc.) affecting the unprivileged population. Harvesting personal data is valuable to cyber criminals as it allows them to impersonate and incriminate others for the crimes they carried out. As reported in the print media, such cybercrimes have been on rise in Pakistan and thus this addresses an urgency to revise the national cybersecurity policy as per global cybersecurity norms.**

Keywords— Cybersecurity, Risk, Privacy, Cybercrime, Laws, Regulations, Policy

I. Introduction

Looking at the pace at which emerging and immersive technologies are embedded to sustain the data-driven digital economy, is has become essential to be aware of the cybersecurity risks associated with it [1], [2]. Pakistan is a developing nation, being the eight-largest exporter for textile and agricultural producer across the world [3]. Besides this, the country is widely known for exporting sports goods and chemicals. As per statistics in [4], the nation's manufacturing output increased by 20% in 2022 and crossed the $49 billion mark. From a manufacturing and agricultural point of view the figures provided seem impressive, however the shortcomings related to the literacy rates cannot be ignored either, 40% of the country's population is uneducated [5], having limited or no access to primary education has been an on-going challenge. Despite of various Government measures in place to combat this situation, many children opt out of primary schools to financially support their families and as per [6], 3.3 million children are deprived of their childhood, basic healthcare and education. The biggest thought here is: how can anyone expect an under privileged generation to understand and be aware of the risks associated to advanced technologies? And in present times, these are the people who suffer the most, get tricked through social engineering (phishing, click-baiting, pharming, tailgating, etc.) [7], [8] and impersonation crimes. In 2023, DAWN [9] highlighted the increasing numbers of financial frauds, victims presumed the malicious actors were accomplice with bank employees and facilitated the frauds. The caller would impersonate as a bank employee, have access to the victims personally identifiable information (PII) and provide account details, previous transactions, etc. for building authenticity of the call and then bait them through it. These types of increasing cyber crimes shed a light on pressing cybersecurity issues such as: lack of strong cybersecurity policies, standards, data governance, risk and controls [1]. A hyper-connected immersive and intelligent environment highly relies on enabling networks, communication systems and technologies for driving the digital economy. To de-escalate the impacts and scale of increasing cybercrime, the first steps are to fully understand and analyze the source of threats/risks arising. Building a robust cybersecurity strategy, policy and standards implementation enables in precisely identifying, assessing and mitigating novel threats/risks arising in cutting-edge technologies, fostering digital and operational resilience. This paper is divided as follows: section II discusses the emerging cyber threat landscape and security challenges in Pakistan, section III focuses on the data privacy, security issues in enabling technologies and their implications, section IV discusses cyber policy and diplomacy and section V concludes the paper.

II. Demystifying Pakistan's Cyber Threat Landscape

The costs of cyber crime is increasing by 15% each year and by 2025 it is anticipated to touch the $10.5 trillion mark, surpassing the world's largest economies [10]. Having the ability to operationally, financially, politically disrupt an economy and cause social unrest in a Country is the biggest cyber threat. The impact of mis-information and dis-information spread across social media handles can develop chaos in matter of minutes. Lack of cyber knowledge and understanding among the wider population and unprivileged, pose national risks that the country must be prepared to mitigate and control. To understand Pakistan's cyber threat landscape it is important to first identify the diversity of elements (illustrated in Fig. 1) that may potentially impact it.

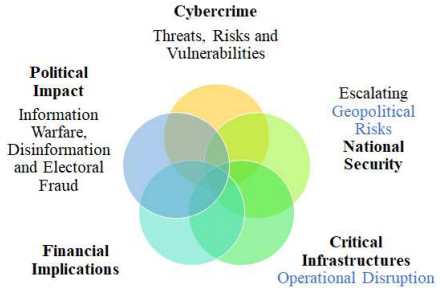

Fig. 1. Comprehensive Cyber Threat Landscape

A. Cyber Crime and National Security

A criminal activity carried out for personal or financial gain (i.e., digital identity fraud, espionage, eavesdropping, cyber-extortion) is classified as a cybercrime [11]. Different malicious actors (hackers) carry different intentions such as: state-sponsored threat actors have the intent to trigger geo-political risks, where as cybercriminals look out for financial gains [2]. Hacktivists are generally ideological threat actors, whereas insider threat actors could be former/current employees holding a grudge against the employer. Different threat actors may have different intentions and skill-sets, abilities to carry out the designated scale of attacks [2], [11]. Cybercrimes have a huge impact on both internal and external shock scenarios [12] and can lead to Denial of Service (DoS), loss of command and control and operational disruption scenarios. Kaspersky and Titan Rain were the most famous state-sponsored cyber attacks that infiltrated exploited and compromised areas related to national security and critical infrastructures [13]. Kaspersky had a global impact whereas Titan Rain impacted US and UK Government agencies. The lesson to learn here is if progressed Nations having strong cybersecurity measures in place can suffer high-risk cyber attacks, then the possibilities of cyber-attacks being carried out without being identified/noticed in developing nations are even higher. As mentioned in [14], lack of security standards and advanced cyber forensics tools, led to increased passive cyber attacks in legacy Industrial Control Systems (ICS). The attacks remained unnoticed for up to 3 to 6 months and by the time they were identified, the damage was already done [14]. Such risks are escalating on daily basis. The more connected and converged an environment is, the more susceptible to is to the emerging threats arising from 5G-IoT, Cloud, biometric data breaches and misuse of Generative AI [15].

B. Critical Infratructures

Critical infrastructure such as: electricity, transportation, communications, defense, agriculture, dams, manufacturing, etc. play an essential role for a society to function at its most. If integrity of any of these environments is compromised it has the potential to cause a domino effect disrupting the economy. As per reports in [16], high-impact attacks on critical infrastructures have increased by 140% and if such risks are not deescalated then 15,000 industrial sites would be forced to shutdown by 2027. Majority of critical infrastructures across the world including Pakistan rely on ICS legacy systems, which if exploited may lead to an immediate down time. Old legacy systems were not devised with security and privacy by design, so the biggest challenges with these interfaces has been to securely extract data from them. Lack of patch management, unencrypted data transmission between internal remote connections, information and operational technology (IT/OT) convergence issues, scattered remote connections (i.e., sensors, plc, etc.), all of these are on-going ICS/OT challenges presently. The Stuxnet cyber-attack showed that air-gapping critical infrastructures was not enough to protect the environment from exploitation [13], [14]. Protecting such infrastructures requires an effective cybersecurity strategy based on the environments IT/OT blueprint, understanding of technological, architectural and third-party dependencies for securing the end-to-end (E2E) flow of data [14]. Safeguarding measures also involve implementing security controls providing assurance of the confidentiality, integrity and availability (CIA) of data, mission-critical-assets being intact at the physical, network, cloud, end-point, perimeter and application levels [14]. In fact additional measures for preventing risks associated to supply-chain and human element may need to be established as well.

C. Financial Implications

Financial cybercrimes occur when malicious actors gain unauthorized access to critical assets and steal information. Alike other industries, financial firms (banking, fintech, insurance, etc.) have also been subjected to increased cyber attacks (malware, phishing, compromised credentials, etc.) as well. The average cost of data breach depends on the records/amount of data stolen and the level of personal information those records could provide [2]. Besides this, the firms would suffer regulatory, legal and reputational damages as well. In the European Union (EU) [2], [11] there are strong regulations such as: (i) General Data Protection Regulation (GDPR) for protecting personal data, (ii) Digital Operational Resilience Act (DORA) for mitigating Information and Communication Technology (ICT) risks, (iii) Cyber Resilient Act (CRA) [1], [2] for implementing hardware and software products security requirements minimizing third-party and supply-chain risks, (iv) Network and Information Security Directive (NIS2-D) for building strong security, legal measures and cyber resilience in critical infrastructures. Financial institutions that fail to comply with the provided mandatory (legal, statutory and regulatory) laws and regulations are subjected to penalties. In 2022, over 900,000 cyber incidents took place in Pakistan, these incidents have reportedly increased in 2023 [17]. The Federal Investigation Agency (FIA) National Response Centre for Cyber Crime in Pakistan [18] mentions reporting and cyber prevention tips on their website, however looking at the country's statistics, where around 64% of the population lives in rural areas and literacy rate is nearly 58% [5], these metrics highlight that the rural and wider population is not literate to understand and be aware of the growing cyber risks associated to banking frauds. Such populations would be the most vulnerable ones. As mentioned in the introduction section, the increasing financial/banking frauds in Pakistan are rising and demonstrate valid concerns related to proper implementation of security (administrative, physical and technical) measures in place. It also underlines negligence and non-compliance with aligning and employing adequate levels of cybersecurity standards, risk mitigation, auditing and controls. With the proliferating cyber-threats, baseline security measures cannot be considered sufficient for protecting such environments from highly sophisticated and advanced attacks. In present times, the biggest challenges are to identify cyber attacks launched from remoted locations and the threat actors behind it. The art of

cyber warfare [13] mentions that majority of such offenses are state-sponsored and carried out by countries bearing on-going sanctions (i.e., Unit 121, Lazarus Group, etc.) with the intention to strengthen their economy and/or to disrupt the adversaries economy. In the past few months Pakistan's currency has dropped against foreign currencies, the economy is also impacted by IMF loans [19], so from a financial perspective, there are high-stakes involved here for protecting the financial institutions and 0% margin for error.

D. Political Impact

A data-driven digital economy highly depends on the reliability of data and if that falls in the wrong (cyber criminals) hands, it has the ability to disrupt the strongest economy. Misuse of generative AI has presented number of examples (i.e., misinformation, deep-fake and advancing hate-crime) [2], [15]. Misleading in forms of advanced dis-information (deceptive information spread with malicious intent), mis-information (false information that may or may not have a malicious intent) have increased geo-political risks [1]. Besides this, jeopardizing national elections by tampering electronic voting systems and outcomes is a matter of concern for national security and a growing cyber threat [20]. Many countries have suffered electoral fraud (unauthorized access, manipulating e-votes with/without the voters consent impacting the integrity, etc.), including the UK Election 2021 [21] and the US Election 2016 [22], both were tampered by external interferences. An article published in [23] mentions integrity as the core foundation for democracy and for a society to function well, transparency and integrity are mandatory. United Nations [24] also supports and states informational warfare, disinformation campaigns and electoral fraud as the key issues that need to be controlled, as their impacts could foster national disabilities. Pakistan, a land that is rich in culture, languages, diversity (population from different ethnicities and races), where an insignificant fake news spread through online/social platforms could originate national unrest (increased crime) in matter of minutes, this is why it is essential to have controls for dis-informational resilience. Closing down communications or internet may not stop dis-information instead hinder freedom of speech [25]. The Cyber Peace Institute has taken initiatives for mitigating dis-information from different angles (i.e., investigating harmful content fostering opportunities for cyber attacks, identifying advanced persistent threat (APT) groups and state sponsored actors using the same tactics, techniques and procedures, tools and infrastructure for carrying out the cyber attacks) [25]. To combat and de-escalate such risks, a country needs to have highly specialized cybersecurity teams and build cyber diplomatic relations with its allies as well.

III. Data Privacy And Security

The 2030 UN Sustainable development goals 4 (quality education), 8 (decent work and economic growth), 9 (infrastructure, innovation and infrastructure), 11 (sustainable cities and communities) and 16 (peace, justice and strong institutions) [24] support the necessities for building a digital economy, however, one of the main factors to achieve these depends on highly secured ICT. The data-driven industries depend on data analytics for providing effective and informed decisions in critical infrastructures, if the data is compromised it can lead to high-risk scenarios such as: nefarious abuse (misusing, altering, stealing information, targeting ICT systems, network and infrastructure compromising the CIA) of the environment [2], [11], [14]. To build cyber resilience, it is essential for critical infrastructures and organizations to implement strong controls enabling data privacy and security [1]. Data privacy refers to proper use and handling of personal data, there are certain data privacy rules that govern how data is collected (consent and purpose), processed (on-premises, cloud), securely shared (encrypted, pseudonymized) when legally required, retained (duration), used and securely destroyed when it is no longer required [1], [2], [8]. There would be even stronger regulatory and governance policies that may apply depending on the level of personal/sensitive information involved. Whereas data security must provide guarantee of E2E Security (CIA of data remains intact) while the data is in-transit, in-use and/or in-storage [14]. Depending on the type of infrastructure, applications, connectivity, communications and technological dependencies, different tools and techniques will be required for securing data such as: (i) policy management (encryption techniques, zero trust, remote access, identity and access management), (ii) data classification and data loss prevention strategies, (iii) patch management, (iv) intrusion detection and prevention tools, next generation firewalls, monitoring and response (security information and event management (SIEM), security orchestration, automation and response (SOAR)), (v) application security, (vi) threat intelligence, (viii) end-point security, etc. [8], [14], [26]. In cybersecurity one standard or solution cannot not fit all, as each organization/infrastructure is different and will require a different cybersecurity strategy. As per [27], more than 8.2 billion data records were globally breached in 2023. *"The growing cyber threats have made it essential to protect personal, sensitive (i.e. genomic, etc.) data where ever and whenever it is used. 99.9% of human race shares an identical genome and the remaining 0.1% holds vital health information"* [28]. Generally this information when collected by healthcare facilities or research centre's is anonymised or pseudonymised for protecting the PII. The Anthem medical data breach in 2015 was an eye-opener in which data related to specialized officers was breached and only discovered during an Audit [13]. The health insurance firm's IT systems were infected and millions of PII records were stolen via a Spyware [13]. This gave malicious actors access to health conditions of each officer and were able to compromise them, such risks are continuously rising [13]. Recently, the genomic company 23andMe [29] that collected genetic material for ancestry and genetic predisposition suffered a breach as well affecting 6.9 million people. Public Services in Pakistan such as: NADRA family tree, check my NIC [30], need to have strong security controls in place because exploitation of SMS services could potentially lead to extended data breaches compromising identities and locations of the general public. Threat actors with criminal intent can misuse this data causing harms to privacy, property, digital identity and financial frauds, affecting the wider population.

Lack of cyber awareness promotes cybercrime as well, millions of people still rely on professional photography studios for passport-sized photographs, once a photo is captured, it is stored on the studios computer, printed and handed-out to the customer. Now, as this data is no longer related to the photographer, he/she must delete this data (photo), and if for some reason he/she needs to retains it, the

studio must have strong identity and access controls in place so that unauthorized people could not have access to it. The photographs captured are generally are of good quality and if they fall into the wrong hands, they can be regenerated by criminals with a bad intent (i.e., deep-fake, digital identity fraud, etc.). The initial draft on Data Confidentiality: Identifying and Protecting Assets Against Data Breaches (NIST SP 1800-28 standard) [31] provides guidance and best practices to organizations for developing data prevention and recovery mechanisms. It also helps organizations in identifying and protecting assets against data confidentiality attacks, including cyber security and privacy considerations that organizations must be cyber-prepared for and technical directions for implementations [31]. Pakistan must have an inclusive cyber policy, strategy and have robust measures in place for enforcing the statutory, regulatory, data security and privacy laws for safeguarding critical and public-facing infrastructures. Non-compliance with these measures must impose heavy fines, enforcing public and private organizations to take mandatory actions for implementing these controls.

IV. Cyber Policy

A cybersecurity policy lays out legal regulations and technical guidelines that the critical infrastructures or organizations must follow for building compliance, minimizing risk and having a technical incident response in place [32]. A policy helps in enforcing high-level measures for safeguarding critical-assets against cyber attacks and data breaches. For a digital economy to succeed it is mandatory to have a cyber policy for protecting the growing and new businesses, fostering a safe, transparent and sustainable cyber ecosystem. There are different parts that play a critical role in designing an effective cyber policy and are discussed below:

A. Demystifying potential factors influencing cyber policy

Living in the Web 4.0 era, it is essential for the internet to be a secure and transparent space for all [33]. The WEF report indicates the complexities and interconnectivities with the different dimensions of the society and their impact, if one link is exploited it could easily trigger or escalate to a high-level cross-border risk and this is why it is important to demystify the cyber threat landscape using the Political Economic Social Technological Legal and Environment (PESTLE) factors [33], [34]. PESTLE demonstrates external variables impacting and influencing organization's/critical infrastructures operations and policies. Fig. 2 presents the PESTLE factors influencing Pakistan's cyber policy.

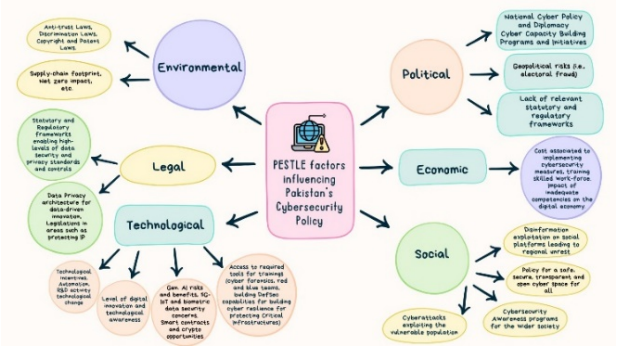

Fig. 2. PESTLE factors influencing Pakistan's Cybersecurity Policy

These variables can be further classified based on different threats (i.e., misusing ICTs, weaponizing interception, force majeure, unlawful surveillance, accidental damages, physical attacks, etc.) [11]. A disaster/force majeure situation is often overlooked but it can potentially lead to high-impact scenarios (i.e., flooding, earthquakes, weather induced landslides impacting communication lines/signals), fostering social unrest) [14]. Cyberattacks carried out on critical infrastructures (electricity, aviation, etc.) directly impacts human lives, this is why cyber laws, policy and national cybersecurity response teams are important and must always be cyber prepared [35], [36].

B. Developing a policy at the organisational level

An organization may have their own legal team for helping them in incorporating the essential components from the national policy in their organizational cyber policy. There are various external and internal factors (as shown in Fig. 3) influencing the cyber policy (i.e., external influencers can be statutory, regulatory or contractual requirements) and may impose penalties in situations of non-compliance, this aspect is also tied up with control objectives for assurance that the defined level of security measures are being met [32]. Whereas at internal level a policy can be influenced by the board of directors, corporate policies, etc. with the aims to ensure that the organization is meeting the defined objectives and has its scope aligned with the business strategy.

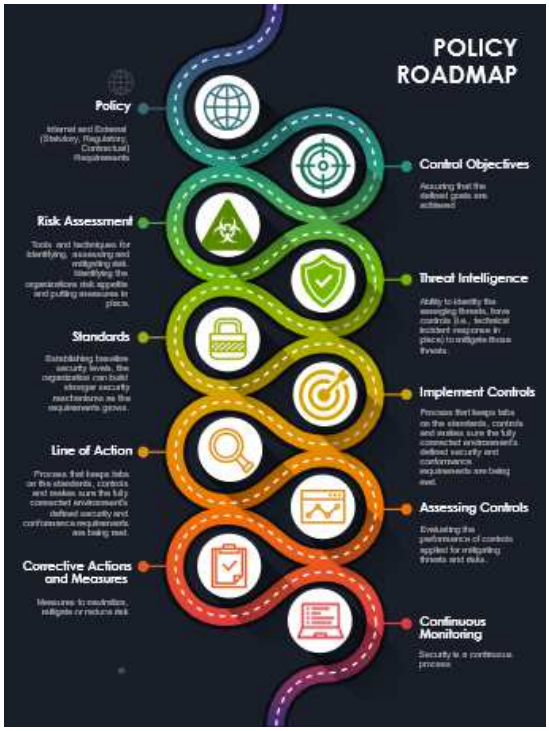

Fig. 3. Author designed Policy Roadmap adapted from [32]

Policies are implemented using cybersecurity standards. The statutory and regulatory laws also embedded at the policy level, these mandatory laws set the requirements for protecting data. The contractual standards are generally implemented to provide assurance to customers that the organization has appropriate level of security measures in place [32]. Once a policy is developed, the Control Objectives (CO) are aligned to meet the defined policies. COs provide due diligence and measures whether a desired outcome is achievable or not [32]. The next steps involves

assessing the risks using qualitative and quantitative methods, building threat intelligence, aligning and implementing relevant standards for monitoring/controlling the threats/risks. Each standard is mapped across the CO and technical, administrative, physical controls. Policies require a line of action (LOA) to inspect the standards and controls implementation from a compliance perspective. LOA also keeps tabs on the tasks assigned to relevant roles, actions items and workflow. This process directly feedbacks to the controls for keeping the threats/risks at minimal, acceptable and tolerable levels. This would include assessing the controls, checking their efficacy, looking into audits and monitoring the residual risk. Any gaps or escalating risks detected at this stage lead to corrective actions. Once the risks are treated/controlled, the process must be continuously monitored. Each organization may have their own way to implement a policy, majority of the processes would be cross-functional to make the policy agile and adaptable for mitigating cyber governance, risk and control issues [32].

To successfully implement policies at organizational level, establishing clear and comprehensive guidelines is essential for the workforce, third-party and stakeholders involved with handling critical IT/OT assets and data to follow (e.g., if an organization requires a data management policy, it must provide guidelines on data governance, risk and control) [32]. Human risks have been continuously increasing, so the policies must include capacity building and workforce training programs. The cybercrime competency framework by Europol [37] provides a comprehensive matrix across cyber roles, skill-set and expertise of Law Enforcement Authorities and judiciary practitioners engaged in the field of cybercrime and digital investigations. Organizations must review and update their policies with the changing cyber threat landscape.

C. Designing an International ot Nation-wide cyber policy

A national cyber policy plays an instrumental part for firms in designing their local policies at the public/private organization levels [32]. For countries who are in-process and striving for excellence in the cyber domain may learn from Nations who have already developed strong cybersecurity policy such as the European Union (EU). As per [38], the EU addresses the urgency for building cyber-resilience, safeguarding data and communications protecting the economy and online community [38]. EU's cybersecurity strategy further focuses on building joint cyber capability and capacity building initiatives, certifications, standards for securing and stabilizing the cyberspace [38], [39]. Various legislations have been in place such as: NIS2-D, CRA, Cybersecurity Act, Cyber Solidarity Act for improving the response to cyber threats across the EU [1], [2], [38]. The EU plans to incorporate a cybersecurity shield (a complete cyber combat mechanism) for developing a strong cyber defense system [38]. High-level cybersecurity and ICT certifications established by ENISA provide strong standards implementations and development of a common EU certification system [38]. The policy also shares light on mitigation plans for large-scale cross-border crisis, EU joint cyber task force and electoral process security, etc. Initiatives related to cyber diplomacy and cyber issues have been linked to the foreign and security policies, implementation of International Law, strategic alliances on norms and confidence building measures [39]. The Cyber Diplomacy Toolbox is a *"joint EU diplomatic response to malicious cyber activities (i.e., proportional to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity). The diplomatic efforts promote security and stability on the web through increased collaboration, cooperation, provides clarity and reduces the risk of confusions and conflict stemming from ICT incidents"* [39]. The EU's Digital Decade 2030 policy aims to ensure *"human rights protection, democracy, and that all digital players act responsibly and safely, freedom of choice (having a fair online environment, safe from illegal and harmful content, that can be empowered while interacting with new and emerging technologies, ensuring safety and security to users for all ages, bridging the gaps (enabling solidarity and inclusion), fostering participation (facilitating participation in the democratic process at all levels and control over their own data and building sustainable devices supporting the green transition"* [40]. New regulations (i.e., Chip Act, Digital Product Passport, etc.) [2], [39], [41] are being developed to combat the emerging threats such comprehensive cybersecurity strategy and policy provides a roadmap to all public/private entities across Europe.

D. Pakistan's National Cyber Crime Policy and Laws

A cyber policy is critical part of the digital economy as it plays a vital role in regulating all aspects of digital ecosystem. In a free democratic society, cyber policy presents novel challenges (i.e., national security, business interests weighed against freedom of speech, privacy and accessibility concerns) [42]. Pakistan's National cyber crime policy 2021 [43], [44] draft requires strong and exceptional measures for addressing and mitigating the emerging global cyber threats that may have an impact on the country's national security. *Majority of the policy deliverables are directly linked to cybersecurity and objectify a governance and institutional framework for the secure the functionality of public and private organizations in compliance"* [44]. The Cybersecurity Strategy for Telecom sector (2023-2028) [45], provides a roadmap for implementing the National Cyber Crime Policy 2021 over the next 5 years (2023-2028) and tactically focuses on the following areas: (i) legal framework, (ii) cyber resilience, (iii) proactive monitoring and incident response (iv) capacity building (v) co-operation and collaboration across national and international organizations, computer emergency response team (CERT), other sector regulators, academia (vi) and most importantly end-user and organizational cyber awareness goals. CERT 2023 [45] includes team formation, functionality and competencies, implementing and measuring the key performance indicators. The Prevention of Electronic Crimes Act (PECA) 2016 [46] of Pakistan is a statutory law that applies to the whole country and if any cybercrime is committed from outside the territory affecting the CIA of data, information systems, brings harms to people or property/critical infrastructures, the malicious actor/actors would be convicted/prosecuted based on PECA 2016. The Act also associates with related legislations and codes such as: Pakistan Telecommunication (Re-organisation) Act 1996, Code of Criminal Procedure 1898, Pakistan Penal Code 1860). PECA 2016 [46], chapter II refer to the offenses and punishments, chapter III shares insights on the federal legal powers to investigate (digital forensic, etc.), chapter IV focuses on international cooperation, chapter V Prosecution and trial of offences and chapter VI outlines the preventive measures. Even though these laws are enacted in Pakistan for protecting cyber crimes, there is a great need for a comprehensive

framework/roadmap for implementing these measures at the micro and macro-levels, only then nation would be able to prepared and assess its cyber readiness index.

Given the current situation, there is an urgent need for data governance, risk and controls for protecting public's personal data. With the escalating cyber threats, developing nations have been actively revising their cyber policy, this is a food for thought for reviewing Pakistan's cyber policy with a present foresight. For a digital economy to prosper it is essential that mandatory security measures are enforced across public/private/critical infrastructures. A suggestion would be mandating implementing the statutory and regulatory laws, cybersecurity standards and risk controls. The implementation would be taken seriously if implications (penalties) for non-compliance are posed. The cybersecurity strategy must deliver a thorough policy framework ensuring effective implementation safeguarding local, national and international interests.

V. Conclusion

Success of a data-driven digital economy and broader society relies on the security and privacy of data. This can be achieved through proper implementation of cybersecurity standards, regulations and policies at the national and organizational levels. Policies have a huge impact on people's daily lives as it provides a roadmap for understanding the processes in place for protecting data, assets and organizations. This paper shares insights on the emerging cyber threat landscape, data security and privacy challenges, cyber crimes, existing laws and strongly suggest needs for robust measures towards reviewing of Pakistan's cyber policy and strategy. In addition there is a dire need enforcing the statutory, regulatory, cybersecurity standards and laws for safeguarding critical and public-facing infrastructures, building operational resilience, cyber awareness and measures for non-compliance protecting the wider population from harm.

References

[1] H. Meagher and L. L. Dhirani, "Cyber-Resilience, Principles, and Practices," *Internet of Things*, vol. Part F1832, pp. 57–74, 2024, doi: 10.1007/978-3-031-45162-1_4.

[2] L. L. Dhirani, N. Mukhtiar, B. S. Chowdhry, and T. Newe, "Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review," *Sensors 2023, Vol. 23, Page 1151*, vol. 23, no. 3, p. 1151, Jan. 2023, doi: 10.3390/S23031151.

[3] "Textile | Board Of Investment." Accessed: Jan. 27, 2024. [Online]. Available: https://invest.gov.pk/textile

[4] "Pakistan Manufacturing Output 1960-2024 | MacroTrends." Accessed: Jan. 27, 2024. [Online]. Available: https://www.macrotrends.net/countries/PAK/pakistan/manufacturing-output

[5] "Pakistan 2023 IFRC network country plan (MAAPK002) - Pakistan | ReliefWeb." Accessed: Jan. 27, 2024. [Online]. Available: https://reliefweb.int/report/pakistan/pakistan-2023-ifrc-network-country-plan-maapk002

[6] "Various measures already in place, experts stress elimination of child labour in Pakistan | Pakistan Today." Accessed: Jan. 27, 2024. [Online]. Available: https://www.pakistantoday.com.pk/2023/06/11/various-measures-already-in-place-experts-stress-elimination-of-child-labour-in-pakistan/

[7] "Phone scams to data leaks: securing Pakistan's digital frontier." Accessed: Jan. 27, 2024. [Online]. Available: https://tribune.com.pk/story/2444854/phone-scams-to-data-leaks-securing-pakistans-digital-frontier

[8] M. A. Khatun, S. F. Memon, C. Eising, and L. L. Dhirani, "Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation," *IEEE Access*, vol. 11, pp. 145869–145896, Dec. 2023, doi: 10.1109/ACCESS.2023.3346320.

[9] "PAKISTAN'S WEB OF CYBER SCAMMERS - Newspaper - DAWN.COM." Accessed: Jan. 27, 2024. [Online]. Available: https://www.dawn.com/news/1764628

[10] "2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics." Accessed: Jan. 27, 2024. [Online]. Available: https://cybersecurityventures.com/cybersecurity-almanac-2023/

[11] ENISA Foresight Cybersecurity Threats for 2030 — ENISA." Accessed: Jan. 27, 2024. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

[12] "Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment - Carnegie Endowment for International Peace." Accessed: Jan. 27, 2024. [Online]. Available: https://carnegieendowment.org/2019/09/30/cyber-risk-scenarios-financial-system-and-systemic-risk-assessment-pub-79911

[13] J. DiMaggio, "The art of cyberwarfare : an investigator's guide to espionage, ransomware, and organized cybercrime," p. 254, Accessed: Jan. 27, 2024. [Online]. Available: https://books.google.com/books/about/The_Art_of_Cyberwarfare.html?id=HxZOEAAAQBAJ

[14] L. L. Dhirani, E. Armstrong, and T. Newe, "Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap," *Sensors 2021, Vol. 21, Page 3901*, vol. 21, no. 11, p. 3901, Jun. 2021, doi: 10.3390/S21113901.

[15] "Securing 5G and IoT in the Energy and Healthcare Sectors." Accessed: Jan. 27, 2024. [Online]. Available: https://itegriti.com/2023/cybersecurity/securing-5g-and-iot-in-the-energy-and-healthcare-sectors/

[16] "High-Impact Attacks On Critical Infrastructure Climb 140%." Accessed: Jan. 27, 2024. [Online]. Available: https://securityintelligence.com/news/high-impact-attacks-on-critical-infrastructure-climb-140/

[17] "Is cyber-security important to Pakistan?" Accessed: Jan. 27, 2024. [Online]. Available: https://tribune.com.pk/story/2383197/is-cyber-security-important-to-pakistan

[18] "National Response Centre For Cyber Crime." Accessed: Jan. 27, 2024. [Online]. Available: https://www.nr3c.gov.pk/

[19] "IMF board approves $700 mln loan as part of Pakistan bailout | Reuters." Accessed: Jan. 27, 2024. [Online]. Available: https://www.reuters.com/markets/asia/imf-board-approves-700-mln-loan-part-pakistan-bailout-2024-01-11/

[20] "Electoral Commission failed cybersecurity test in same year as hack | Electoral Commission | The Guardian." Accessed: Jan. 27, 2024. [Online]. Available: https://www.theguardian.com/politics/2023/sep/05/electoral-commission-failed-cybersecurity-test-in-same-year-as-hack

[21] S. Farrall, S. Wilks-Heeg, R. Struthers, and E. Gray, "Who are the victims of electoral fraud in Great Britain? Evidence from survey research," *British Politics*, vol. 17, no. 3, pp. 333–352, Sep. 2022, doi: 10.1057/S41293-021-00189-1/TABLES/5.

[22] "Office of Public Affairs | Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election | United States Department of Justice." Accessed: Jan. 27, 2024. [Online]. Available: https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

[23] "Online misinformation and foreign interference fears for this year's elections." Accessed: Jan. 27, 2024. [Online]. Available: https://www.irishexaminer.com/news/arid-41300275.html

[24] "Transforming our world: the 2030 Agenda for Sustainable Development | Department of Economic and Social Affairs." Accessed: Jan. 27, 2024. [Online]. Available: https://sdgs.un.org/2030agenda

[25] "Home | CyberPeace Institute." Accessed: Jan. 27, 2024. [Online]. Available: https://cyberpeaceinstitute.org/

[26] "Top 7 types of data security technology | TechTarget." Accessed: Jan. 27, 2024. [Online]. Available: https://www.techtarget.com/searchsecurity/feature/Top-7-types-of-data-security-technology

[27] “List of Data Breaches and Cyber Attacks in 2023 – 8,214,886,660 records breached - IT Governance UK Blog.” Accessed: Jan. 27, 2024. [Online]. Available: https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023

[28] “Genomic Data Science Fact Sheet.” Accessed: Jan. 27, 2024. [Online]. Available: https://www.genome.gov/about-genomics/fact-sheets/Genomic-Data-Science

[29] “The 23andMe data breach reveals the vulnerabilities of our interconnected data.” Accessed: Jan. 27, 2024. [Online]. Available: https://theconversation.com/the-23andme-data-breach-reveals-the-vulnerabilities-of-our-interconnected-data-193615

[30] “How to get family tree from Nadra in 2023 - NADRA Box.” Accessed: Jan. 27, 2024. [Online]. Available: https://www.nadrabox.com/2023/01/how-to-get-family-tree-from-nadra-in.html

[31] W. Fisher, R. Craft, M. Ekstrom, J. Sexton, and J. Sweetnam, “Data Confidentiality: Identifying and Protecting Assets Against Data Breaches.” Dec. 13, 2023. Accessed: Jan. 27, 2024. [Online]. Available: https://csrc.nist.gov/pubs/sp/1800/28/ipd

[32] ComplianceForge, “ComplianceForge Reference Model - Hierarchical Cybersecurity Governance Framework (HCGF),” 2023, Accessed: Jan. 27, 2024. [Online]. Available: https://www.complianceforge.com/grc/hierarchical-cybersecurity-governance-framework/

[33] “Global Risks Report 2024 | World Economic Forum | World Economic Forum.” Accessed: Jan. 27, 2024. [Online]. Available: https://www.weforum.org/publications/global-risks-report-2024/

[34] L. Tähtinen, S. Toivonen, and A. Rashidfarokhi, “Landscape and domains of possible future threats from a societal point of view,” *Journal of Contingencies and Crisis Management*, vol. 32, no. 1, p. e12529, Mar. 2024, doi: 10.1111/1468-5973.12529.

[35] B. Mazanec and C. Whyte, “Understanding Cyber-Warfare : Politics, Policy and Strategy,” *Understanding Cyber-Warfare*, Apr. 2023, doi: 10.4324/9781003246398.

[36] J. F. Lancelot, “Cyber-diplomacy: cyberwarfare and the rules of engagement,” *Journal of Cyber Security Technology*, vol. 4, no. 4, pp. 240–254, Oct. 2020, doi: 10.1080/23742917.2020.1798155.

[37] “Europol PUBLIC Information Cybercrime Training Competency Framework”. Accessed: Jan. 27, 2024. [Online]. Available: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Cybercrime%20Training%20Competency%20Framework%202024.pdf

[38] “Cybersecurity Policies | Shaping Europe’s digital future.” Accessed: Jan. 27, 2024. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

[39] “The EU Cyber Diplomacy Toolbox.” Accessed: Jan. 27, 2024. [Online]. Available: https://www.cyber-diplomacy-toolbox.com/

[40] “Europe’s digital decade: 2030 targets | European Commission.” Accessed: Jan. 27, 2024. [Online]. Available: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

[41] “Digital product passport: A ticket to brand sustainability?” Accessed: Jan. 27, 2024. [Online]. Available: https://www.siliconrepublic.com/enterprise/digital-product-passport-eu-commission-green-sustainability-clothing

[42] “What is Cyber Policy and Why is it Important? | Utica University Online.” Accessed: Jan. 27, 2024. [Online]. Available: https://programs.online.utica.edu/resources/article/what-is-cyber-policy

[43] “Pakistan’s Cybersecurity Policy in 2021: A Review.” Accessed: Jan. 27, 2024. [Online]. Available: https://www.isaca.org/resources/news-and-trends/industry-news/2021/pakistans-cybersecurity-policy-in-2021-a-review

[44] “Government of Pakistan National Cyber Security Policy 2021”. Available: Accessed: Jan. 27, 2024. [Online]. https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf

[45] “CYBER SECURITY STRATEGY FOR TELECOM SECTOR 2023-2028.” Accessed: Jan. 27, 2024. [Online]. Available: https://pta.gov.pk/assets/media/cyber_security_strategy_telecom_sector_2023_2028_13-12-2023_1.pdf

[46] “BILL to make provisions for prevention of electronic crimes”. Pakistan, 2016, pp. 1–29. Accessed: Jan. 27, 2024. [Online]. Available: https://na.gov.pk/uploads/documents/1470910659_707.pdf