Strategic Gap Analysis of Palestine Cybersecurity Performance in the Context of GCI, Kingdom of Saudi Arabia Cybersecurity Posture and Anti-Cybercrime Law, and Council of Europe Convention

Amr J. Atrash, Mousa Farajallah, Ibrahim Alsharif, and Nedal R. Shanti

Abstract— **Palestine rapid digital transformation is facing multiple challenges in the field of cybersecurity. An analysis of the Global Cybersecurity Index (GCI) for the years 2017–2024 revealed that Palestine's performance has declined compared to the leading vision of the Kingdom of Saudi Arabia [15][16][28]. This research aims to identify strategic gaps in the Palestinian legal and institutional framework for combating cybercrime (Decree 2018) using a mixed methodology that combines quantitative analysis of GCI data with qualitative comparative analysis of the Saudi Anti-Cybercrime Law (2007) and the standards of the Budapest Convention [6][11][12]. The research uses a parallel design to integrate the results of descriptive and trend data analysis with semi-structured interviews and comparative legal literature [29]. The analysis revealed significant gaps in the legal, regulatory, technical, developmental, and cooperation pillars with shortcomings in updating data protection legislation, reporting mechanisms, and international cooperation, and weak digital forensic investigation capabilities [28]. Accordingly, the research proposes a package of recommendations that includes updating legislation to protect privacy and data, establishing a national cybersecurity authority, enhancing technical and regulatory capabilities, and deepening international partnerships, with a phased timeline for measuring progress using indicators derived from the GCI.**

I. Introduction

Some studies divide the dimensions of human existence into four main axes: the body, the mind, the external world, and the internal world [1]. With the rapid development of digital technologies and the increasing reliance on cyberspace in various aspects of life, cyberspace has come to be viewed as the fifth dimension of human existence, after land, sea, air, and outer space [2]. This concept has crystallized in workshops and international organizations concerned with Internet governance and cybersecurity, such as the Internet Governance Forum (IGF) and the World Summit on the Information Society (WSIS) forums [2].

We become more vulnerable to the evolving risks in cyberspace as we get increasingly digitalized. The very same technology that makes our lives better may also be abused to cause chaos, foster distrust, and widen social gaps. Singapore's Prime Minister is Lee Hsien Loong [3].

The cyber dimension encompasses a wide range of components, including computers, smartphones, networks, and infrastructure for communication-related services and applications. It is a virtual arena in which social, economic, educational, entertainment, and other activities take place, meaning that life in its various manifestations now takes place, partially or entirely, through this space. As digital dependence increases, so do the risks associated with cyber threats, as the same technologies that improve our quality of life can be used to cause harm, undermine trust, and widen social gaps [3].

Protecting cyberspace requires a collective effort at multiple levels, encompassing not only the technical aspect but also the legislative and regulatory framework, national institutions, international cooperation, and community awareness. Governments play a key role in setting policies and overseeing the implementation of measures that ensure a secure digital environment within national borders [3]. Strengthening cybersecurity is a vital factor in supporting the growth of the ICT sector and protecting countries' critical infrastructure, thus enhancing both economic development and national security [4].

On the other hand, enacting appropriate legislation to combat cybercrime is considered an integral part of the national cybersecurity plan, as it contributes to deterring cybercrime and protecting citizens and institutions from digital risks. This also includes regulating the handling of personal data, dealing with privacy violations, reporting breaches, and imposing security standards within the public and private sectors [5].

Furthermore, there are still no unified global definitions of cybercrime, but adopting clear and agreed-upon terminology within national policies contributes to unifying efforts and keeping pace with rapid changes in this field. International legislative models, such as the Commonwealth of Independent States' Model Law on Combating Cybercrime and the Council of Europe's Budapest Convention on Combating Cybercrime,

*Resrach supported by Palestine Polytechnic and Arab American University.

A. A. Author is with the Department of Natural, Engineering and Technology Sciences Faculty of Graduate Studies Arab American University Ramallah, West Bank, Palestine (author phone: 970-598-750557; e-mail: a.atrash5@student.aaup.edu).

M. F. Author is with the Department of Natural, Engineering and Technology Sciences Faculty of Graduate Studies Palestine Polytechnic University, Hebron, West Bank, Palestine (e-mail: mousa_math@ppu.edu).

I. A. Author is with the Department of Natural, Engineering and Technology Sciences Faculty of Graduate Studies Palestine Polytechnic University, Hebron, West Bank, Palestine (e-mail: Ibrahim_Alsharif@ppu.edu).

N. S. Author is with the Department of Natural, Engineering and Technology Sciences Faculty of Graduate Studies Palestine Khadori Technical University Ramallah, West Bank, Palestine (e-mail: nedal.shanti@pass.ps).

978-9950-8599-0-6

demonstrate how to formulate definitions and legal aspects that are consistent with international requirements [6]. The cross-border nature of cybercrime also highlights the importance of coordination between states and international organizations (such as the International Telecommunication Union, the Organization for Economic Co-operation and Development, and others) to narrow legislative gaps and enhance cooperation in investigation and prosecution [2][7][8].

In the context of Palestine, and with the country's move towards digital transformation and the expansion of e-services (e-government, online banking, education, and health services), there is an urgent need to develop a comprehensive cybersecurity framework that ensures Palestinian society benefits from digital advantages while mitigating risks. This research attempts to understand the legal aspects of cybersecurity in Palestine by comparing the Palestinian Anti-Cybercrime Law (promulgated by decree in 2018) with the Anti-Cybercrime Law in the Kingdom of Saudi Arabia as a reference model, guided by international standards, such as the Budapest Convention and the Global Cybersecurity Index (GCI).

The research also reviews the evolution of Palestine's and Saudi Arabia's rankings in the GCI over the past four editions and evaluates Palestine's performance across the five pillars of the index (legal, technical, regulatory, capacity development, and cooperation) to identify strategic gaps and make recommendations for developing a comprehensive national cybersecurity strategy based on Palestine's capabilities, needs, and the priority of protecting its digital sovereignty.

II. Background of Discussion

Technology and cybersecurity in Palestine are emerging and rapidly evolving fields, providing an exceptional opportunity for Palestine to leverage digital transformation to support its economic and social goals and enhance its integration into the global economy while avoiding some of the pitfalls experienced by advanced countries in the early stages of digitization [9][10]. In this context, cybersecurity is considered the cornerstone of any sustainable technological growth, as it acts as an enabling service that supports the development of useful services (such as e-government, online banking, education, and health services). Therefore, emerging countries must join the information society while controlling risk levels, benefiting from the experiences of advanced countries, and avoiding rushing to open digital access before strengthening protection and defense mechanisms [9][10].

In Palestine, with the significant expansion in the provision of digital and electronic services, the need to coordinate the legal and institutional framework for cybersecurity and combating cybercrime is evident. The absence of a comprehensive framework could lead to legal and technical gaps and disrupt digital development efforts, while a clear framework based on international best practices provides a strong foundation for secure digital transformation [5][6]. This research aims to enable Palestinian decision-makers to understand the legislative dimensions of cybersecurity through a comparative study between the Palestinian Anti-Cybercrime Law (issued by decree in 2018) and the Saudi Anti-Cybercrime Law as a reference model, guided by recognized international standards such as the Budapest Convention on Cybercrime [6][11][12].

A. Why Saudi Arabia

The following are the justifications for selecting SAACL as the foundation and benchmark for comparison with other regional laws already in force:

- The Palestinian Anti-Cybercrime Law was issued in 2018, following a period since the Saudi law was issued in 2007. This allows for the benefit of the Saudi experience in implementing legislation and developing the cybersecurity environment in the Kingdom [11][12].
- The Kingdom of Saudi Arabia has achieved advanced regional and global rankings in its commitment to cybersecurity and the development of a comprehensive national system capable of confronting digital threats. This study makes it useful for guiding Palestinian efforts in formulating a national strategy that takes into account the specificities of the Palestinian environment, its capabilities, and the priorities for protecting its digital sovereignty [15][16][28].
- Saudi Arabia has received international recognition for its role in capacity building, policy development, and the establishment of specialized bodies and national cybersecurity initiatives. This provides a practical model that can be emulated in Palestine, taking into account contextual, geographical, and political differences [14][27].

Based on the above, this research focuses on highlighting opportunities for Palestine to integrate digital defense elements early and avoid the pitfalls faced by some other countries, and working to narrow the gaps between Palestinian legislative frameworks and leading international practices. It also seeks to provide practical recommendations for building an integrated national cybersecurity strategy in Palestine, based on an assessment of the current situation and setting priorities according to global performance indicators such as the Global Cybersecurity Index (GCI) and its five pillars: legal, technical, regulatory, capacity development, and international cooperation and “Table I” Illustrates the ranking of Palestine and the kingdom of Saudi Arabia on the latest four versions of the GCI [15][16][28].

TABLE I. RANKINGNGRANKING OF PALESTINE AND THE KINGDOM OF SAUDI ARABIA ON THE LATEST THREE VERSIONS OF THE GCI.

ITU Report		GCI 2017, V2	GCI 2018, V3	GCI 2020, V4	GCI 2024, V5
Palestine Ranking	Regional	N/A	11	15	N/A
	Global	104	101	122	148
KSA Ranking	Regional	N/A	1	1	1
	Global	46	13	2	1

KSA's cyber readiness has improved over the previous few years. As a result, the kingdom is ranked first regionally and first globally in the fight against cybercrime according to the GCI 2024 study, with the next edition, the sixth, expected in 2026.

The research seeks to answer the main question of identifying strategic gaps in the Palestinian legal and institutional framework for combating cybercrime, compared to the Saudi experience and international standards, particularly the Budapest Convention [7] and the results of the Global Cybersecurity Index (GCI) [29]. It also explores possible ways to adapt lessons learned and formulate a comprehensive national strategy that is compatible with the specificities of the Palestinian context.

Second, from a quantitative perspective, the research examines how the performance of Palestine and Saudi Arabia differed across the 2017–2024 editions across the five pillars of the GCI (legal, technical, regulatory, capacity development, and cooperation). It assesses the magnitude of the time gap and the percentages of change in Palestine's scores compared to Saudi Arabia for each pillar, based on official data issued by the ITU [29]. This quantitative dimension aims to describe trends and identify the weakest pillars of Palestinian performance, enabling the identification of reform priorities.

Third, on the qualitative side, the research focuses on the assessment of Palestinian stakeholders—legislative officials, cybersecurity experts, and representatives from the public and private sectors—of the quality of the current legal framework [11] and its ability to be implemented effectively, while identifying the most prominent contextual challenges arising from geopolitical pressures and constraints on digital infrastructure. The research also explores the possibility of adapting some Saudi practices in legislation, organizational structure, or cooperation mechanisms, and how they can be selected and modified to suit Palestine's resources and institutional environment.

Fourth, in accordance with a mixed research methodology, the mixed dimension aims to combine quantitative and qualitative findings to understand how qualitative perceptions and challenges explain the observed quantitative gaps in Palestine's GCI performance, particularly in the legal and regulatory pillars. This will then formulate reform, procedural, and legislative recommendations supported by digital and contextual evidence. Thus, the above paragraphs form the framework for the research questions that will be addressed in detail in the methodology section, from data collection and analysis to interpretation of the results and proposing recommendations aimed at enhancing Palestinian cybersecurity.

III. RESEARCH METHODOLOGY

This research relies on a mixed methodology that combines qualitative and quantitative analysis. Cybersecurity and its related laws require a deep understanding of legal texts and institutional practices (qualitative), while monitoring objective data on countries' compliance through indicators such as the GCI (quantitative). Qualitative analysis provides an understanding of the context, legal frameworks, and stakeholder positions, while quantitative analysis describes performance trends, such as the evolution of GCI scores for Palestine and Saudi Arabia over the past four editions. Combining the two approaches allows for the verification and comparison of results across multiple sources and methods, which increases the credibility of the research.

A. Data Sources

A.1 Qualitative data

- Legislative Texts: Palestinian Anti-Cybercrime Law (Decree of 2018): Full text of the law and related decrees.
- Saudi Anti-Cybercrime Law (SAACL 2007): Arabic or English translations and related implementing decrees.
- International Conventions and Standards: Budapest Convention on Combating Cybercrime (Bridging with International Standards), International Telecommunication Union (ITU) frameworks and guidelines such as the "ITU National Cybersecurity Strategy Guide," and others.
- National Documents and Policies: Palestinian National Strategy Documents, official reports issued by the Palestinian Ministry of Telecommunications and Information Technology, and Saudi reports on cybersecurity strategies.
- Theoretical and Academic References: Academic studies on legal comparative analysis and methodologies to establish an analytical framework for comparing legal systems.
- Literature on cyber performance assessment and indicators, such as the GCI, the nature of data, and how to process it.
- Previous research addressing the Palestinian case in cybersecurity or regional comparative studies.

A.2 Quantitative data

- Global Cybersecurity Index Reports (2017, 2018, 2020, 2024): Obtain overall scores and performance across the five pillars (legal, technical, regulatory, capacity development, and cooperation) for Palestine and Saudi Arabia to compare trends over time.
- Survey Methodology Details: Review the GCI Survey Background Documents to understand how data was collected and how items were weighted to calculate scores.
- Additional Data: Use additional secondary data such as statistics on the number of cybersecurity initiatives, the number of training workshops, the number of accredited bodies, etc., found in official reports.
- Descriptive Statistics and Trend Analysis: Analyze the evolution of scores for each GCI pillar for Palestine and Saudi Arabia over the past four editions.

B. Analytical Framework

Within the framework of comparative legal analysis, the research relies on functional, analytical, contextual, and structural approaches to examine the legislative frameworks in Palestine and Saudi Arabia, starting with compiling and coding legal texts according to definitions, crimes, penalties, procedures, international cooperation, and privacy protection, and then comparing these provisions with the Budapest Convention standards as a reference list [7]. The research also analyzes the effectiveness and appropriateness of the provisions for the Palestinian context, taking into account institutional capacities, geopolitical pressures, and theories of criminal deterrence to assess the adequacy of penalties and procedures without a real investigative and enforcement capacity [29].

In the quantitative analysis, the scores of Palestine and Saudi Arabia across the five pillars of the Global Cybersecurity Index are extracted from ITU reports (2017–2024) and summarized in tables to calculate gaps, plot development curves, and then calculate percentage changes for each pillar [28][25]. The numerical results are then linked to what the legal analysis has revealed to identify the most vulnerable pillars and priorities for intervention, with recommendations based on integrating measurable performance gaps in the GCI with the necessary legislative and contextual reforms.

C. Verification of reliability and academic validity

The study highlights the importance of validation by verifying the consistency of qualitative coding mechanisms and reviewing them with experts and other researchers, as well as using official sources approved for quantitative data (ITU) to ensure credibility, while employing the principle of integration or triangulation between qualitative and quantitative sources as in Mixed Methods methodologies. Ethical considerations focus on respecting the confidentiality of any potential interviews with stakeholders, obtaining clear consents, ensuring transparency in disclosing data sources and assumptions, avoiding bias in analysis, and presenting results objectively [29].

D. Limits of the study

There are limitations related to the difficulty of accessing actual executive information for legislation in Palestine due to geopolitical conditions, digital occupation, and the lack of technical and human resources, in addition to the possibility of legislative updates being issued in the future that would change some of the results, with the emphasis that the research recommendations must be gradually adapted to the actual Palestinian environment and its institutional capabilities, and that the generalization of the results is restricted by the special circumstances and the need to continuously follow up on developments [29].

IV. ANALYSIS

This study aims to assess the dimensions of the quantitative, legal, and institutional gaps in the Palestinian cybersecurity structure compared to the experience of the Kingdom of Saudi Arabia, based on data from the Government Readiness Index (GCI) for the period (2017–2024) and the Budapest Convention, in addition to criminal justice standards and expert interviews for a comparative analysis of legislative texts and the institutional framework, leading to the formulation of strategic priorities and time-bound recommendations to raise Palestine's performance and enhance its capabilities.

A Quantitative Analysis of GCI Data (2017–2024)

The analysis of the scores and rankings for the period 2018–2024 reflects a widening gap between Palestine and Saudi Arabia. The difference in scores increased from 52.7 points in 2018 to 62.7 points in 2024, while the difference in global rankings increased from 88 to 147 [28][25]. This trend indicates that Saudi Arabia's development in cybersecurity infrastructure was much faster than Palestine's, and that the slight improvement Palestine recorded between 2017 and 2018 was not sustained due to the absence of long-term planning.

First, Palestine's decline in ranking is attributed to slow legislation and the lack of adequate institutional technical capacity development. Previous national efforts focused on partially updating legislation without taking into account the establishment of effective implementation mechanisms or internal monitoring indicators, which was reflected in the weakness of the five pillars of legal, technical, regulatory, development, and international cooperation. **Second**, resources must be mobilized to reassess national policies, through:

- Updating legislation to cover emerging technologies, protecting personal data, and requiring reporting of cyber incidents.
- Developing sub-performance indicators derived from the GCI components to measure progress between versions.
- Conducting qualitative interviews with stakeholders to identify reasons for the decline, such as limited capacity, complex infrastructure under digital occupation, and a lack of international cooperation.

B Comparative Legal and Institutional Analysis

The analysis is based on a benchmarking comparison between the Palestinian Anti-Cybercrime Law No. (10) of 2018 and the Saudi Anti-Cybercrime Law (SAACL 2007), based on the Budapest Convention (2001) as an international reference, in addition to criminal justice standards and expert interviews.

B.1 Definitions and Basic Concepts

Palestinian law defines cybercrimes using the terms "information system" and "unlawful access," but lacks definitions related to cloud computing, the Internet of Things, and artificial intelligence. In contrast, the Saudi law contains clear and comprehensive technical definitions with consistent use of the term's "crime" and "punishment," providing a precise reference for implementation [17][18].

B.2 Scope of the Crimes Prohibited

Palestinian law includes several crimes: unauthorized access, eavesdropping, data modification, system disruption, computer fraud and forgery, privacy violation, online child exploitation, and digital terrorism financing, with some lack of detail regarding the role of service providers in evidence preservation and reporting. The Saudi system covers these same crimes, supported by systems for data protection, e-commerce, and critical infrastructure, enhancing the enforcement and integration of provisions. "Table II" summarizes the anti-cybercrime legislation in Palestine and the Kingdom of Saudi Arabia.

TABLE II. A COMPARATIVE ANALYSIS OF CYBERCRIME LEGISLATION IN PALESTINE AND THE KINGDOM OF SAUDI ARABIA

Criterion	Palestine	Saudi Arabia	Key Gaps
Definitions and Concepts	Incomplete for emerging technologies (IoT, AI)	Comprehensive and consistent; clear legal language	Update definitions to cover emerging crimes
Scope of Offenses	Covers basic offenses but limited in integration	Covers basics and integrates with data and other laws	Link cybercrime law with data protection
Penalties and Deterrence Mechanisms	Theoretically deterrent (3–15 years, fines)	Effectively deterrent with real enforcement and high fines	Enhance investigation capabilities and ensure enforcement
Investigation and Prosecution Procedures	General provisions without details for preserving digital evidence	Clear mechanisms for evidence preservation and judicially backed procedures	Add detailed clauses on evidence preservation and reporting
International Cooperation	Vague or missing provisions	Clear provisions and memoranda of understanding with international bodies	Draft legislative framework for cooperation under Budapest Convention
Protection of Fundamental Rights and Privacy	No standalone data protection law	Independent data law + breach notification mechanisms	Enact data protection law and impose mandatory notification
Institutional Framework and Coordination	Absence of an independent national authority	National Authority (NCA) by royal decree with executive powers	Establish a national authority with clear mandates
Integration with Related Laws	Limited: e-commerce, critical infrastructure	Integrated: data, e-commerce, telecommunications	Conduct a comprehensive review of legislation and resolve overlaps

The "Table II" compares anti-cybercrime legislation in Palestine and Saudi Arabia, identifying key gaps in the Palestinian framework. In Palestine, definitions and concepts remain incomplete regarding emerging technologies such as the Internet of Things and artificial intelligence, while Saudi Arabia adopts clear and comprehensive legal language. Palestinian law also covers traditional crimes without sufficient integration with data protection and communications legislation, unlike Saudi Arabia, which has integrated its cybercrime law with data and e-commerce legislation. Although Palestine theoretically provides deterrent penalties (imprisonment from 3 to 15 years and fines), the ability to investigate and enforce sentences remains limited, while Saudi Arabia effectively enacts and enforces penalties with high fines. Procedures for preserving digital evidence and prosecuting perpetrators in Palestine require further detail and judicial translation, while the Saudi side possesses clear mechanisms supported by judicial authority. Palestine must also formulate an international cooperation framework consistent with the Budapest Convention to address the absence or ambiguity of current cooperation provisions. Furthermore, it is necessary to enact an independent data protection law with mandatory notification of breaches, and establish an independent national body with clear executive powers to ensure effective coordination and legislative integration covering vital infrastructure, e-commerce, and telecommunications [6-8],[19].

B.3 Sanctions, Penalties, and Deterrence

Palestinian legislation provides for prison sentences ranging from 3 to 15 years and fines of up to approximately $14,000. As summarized in “Table III” However, limited technical and logistical capabilities for investigation and prosecution weaken the deterrent effect. Saudi Arabia, on the other hand, achieves a stronger deterrent through high fines and prison sentences, supported by a strong institutional structure that ensures effective implementation of the provisions.

TABLE III. GENERAL COMPARISON BETWEEN PALESTINE AND SAUDI ARABIA

Country		Palestine	K.S.A.
Legislation type		Law by Decree	Royal Decree
Promulgation date		2018	2007
Number of articles		57	16
Fines	Min	Not less than 280 USD	133,000 USD
	Max	Not more than 14,000 USD	1,333,000 USD
Imprisonment	Min	Not less than 3 years	Not more than 1 Year
	Max	Not more than 15 years	Not more than 10 Years
Confinement	Min	One week	X
	Max	3 Years	X

The “Table III” provides a quick comparison between cybercrime legislation in Palestine and Saudi Arabia. The Palestinian law was issued by decree in 2018 and includes 57 articles, while the Saudi law was issued by royal decree in 2007 and includes 16 articles. Fines in Palestine range from $280 to $14,000, compared to $133,000 to $1,333,000 in Saudi Arabia. The minimum prison term in Palestine is three years and a maximum of 15 years, while in Saudi Arabia it does not exceed one year. Palestinian law also includes pretrial detention sentences ranging from one week to three years, unlike Saudi Arabia, which does not apply this penalty [23].

The king's name and the president (in the absence of the legislative council) were used to pass the SAACL and PCL, demonstrating the greatest level of commitment to tackling cybercrime. Some theorists contend that deterrents can help governments lower crime rates because they make offenders think twice about committing a crime if they know they risk being caught and face swift and severe punishment. On the basis of this, the global deterrence theory contends that the threat of exile deters crime. Contrarily, the specific deterrence hypothesis contends that harsher punishments are necessary to dissuade criminal behavior [20].

B.4 Investigation and Trial Procedures

Palestinian law lacks detailed provisions on preserving and ensuring the integrity of digital evidence, and suffers from a shortage of experts and training. Saudi Arabia, however, provides specialized units and clear mechanisms for digital investigation and evidence exchange through international agreements. To enhance the effectiveness of procedures, it is necessary to establish specialized digital investigation units in Palestine, and to train judges and tribunals on the rules for preserving digital evidence, reporting methods, and incident response.

B.5 International Cooperation Mechanisms

Palestinian law lacks clear provisions for international cooperation, while the Saudi system includes memoranda of understanding with foreign enforcement agencies and agreements for the execution of judgments and extradition of criminals. Palestine could benefit from the Saudi model by drafting a legislative framework for cooperation in accordance with the Budapest Convention, taking into account the specific political situation and international recognition.

B.6 Protection of Fundamental Rights and Privacy

Palestine lacks independent legislation to protect personal data or mandatory notification mechanisms for breaches, which undermines digital trust. In contrast, Saudi Arabia regulates data protection through a separate law that includes requirements for data preservation and breach reporting, and guarantees individuals' rights to access and rectify data. Therefore, a personal data protection law must be enacted that links the fight against cybercrime with the protection of privacy.

B.7 Institutional Framework and Coordination

Palestine lacks an independent national cybersecurity body with clear executive powers. Saudi Arabia established the National Cybersecurity Authority by royal decree, which is responsible for policy-making, oversight, and coordination among agencies. It is essential to establish a higher cybersecurity body in Palestine with coordination and regulatory powers, linking it to ministries, the private sector, and research bodies, while regulating the relationship with law enforcement agencies to overcome infrastructure constraints.

B.8 Integration with Other Laws

Palestine needs to integrate cybercrime provisions with laws on data protection, e-commerce, critical infrastructure

protection, and intellectual property rights, and issue joint executive regulations that define the responsibilities of agencies in the event of cyber incidents. In contrast, Saudi Arabia has an integrated legislative system that supports the implementation of SAACL by linking it to multiple systems.

C Integrated Consolidation of Results

The quantitative decline in the GCI is partly due to delays in updating the legislative framework and implementing sanctions, and to the lack of technical capacity of institutions. Qualitative interviews reveal that limited human and technical resources, and the complexity of infrastructure under digital occupation, are driving progress backward. Accordingly, the study outlines three priority areas:

- Short-term (6–12 months): Update legal definitions to include emerging technologies and data protection, and impose mandatory reporting of cyber incidents.
- Medium-term (1–3 years): Establish the National Cybersecurity Authority by decree and define its powers, create specialized digital investigation units, and train judges and investigators.
- Long-term (3–5 years): Integrate cybercrime legislation with e-commerce and critical infrastructure protection laws, and conclude bilateral and multilateral agreements to support investigation and enforcement.

These steps are accompanied by periodic monitoring mechanisms based on an annual review schedule and performance indicators (KPIs) drawn from the five GCI components: legal, technical, regulatory, institutional development, and international cooperation. Conclusion

The widening gaps in Palestinian cybersecurity require a comprehensive strategic approach, starting with immediate legislative updates and building technical and institutional capacities, and culminating in the establishment of strong international partnerships and periodic monitoring mechanisms based on GCI indicators. The Saudi experience provides an inspiring model for an integrated development approach, with solutions tailored to Palestinian constraints and realities.

D Additional laws

like the Copyright Act, Trademark Act, Protection of Personal Information Act, Telecom Act Bylaw, and Electronic Transaction Act, are applicable to cybercrime. Essentially, it is advised to combine all Cybercrime and pertinent provisions in a single document rather than having numerous sets of laws with provisions addressing different Cybercrimes [23].

Even though the PCL has recently matured, this does not make it a model role. To recognize the new threats and violence against people (Cyberviolence), which have emerged as a major issue for societies and individuals, some vulnerabilities in the PCL need to be updated and enhanced. Targeting either individuals or groups, cyberviolence can involve a wide variety of offenses [24].

Cyberviolence is broadly defined as "the use of computer systems to cause, facilitate, or threaten violence against individuals that results in, or is likely to result in, physical harm, sexual harm, psychological harm, or economic harm or suffering and may include the exploitation of the individual's circumstances, characteristics, or vulnerabilities" [24].

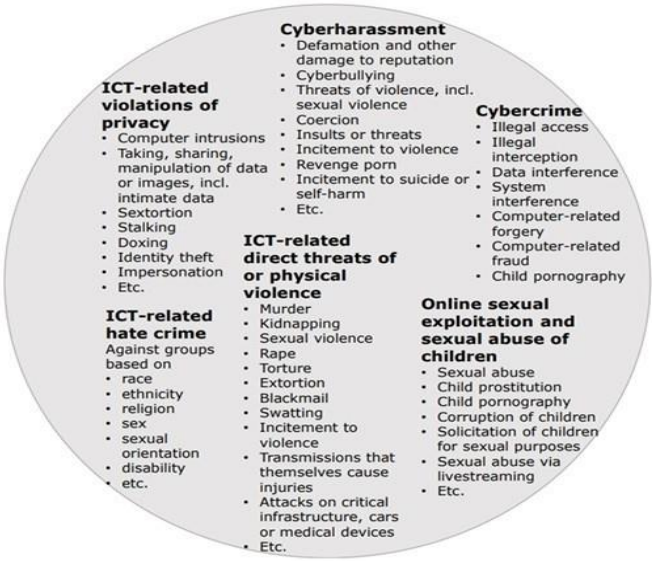

Figure 1. Types of Cyberviolence used by the "Council of Europe's Cybercrime Convention Committee"[24].

GCI divided the world's nations into three groups based on their level of cybersecurity readiness and GCI score [15].

1. The countries in the initiating stage are those whose GCI ratings are below the median and which have begun to take cybersecurity commitments.
2. The term "maturing stage" refers to nations that have GCI scores between the 50th and 89th percentile and have engaged in cybersecurity programs and initiatives, as well as developed complex commitments.
3. The term "leading stage" describes nations with GCI scores in the 90th percentile and who have shown a strong commitment to the GCI index's five pillars.

D.1 Assessment of Palestine's performance on the five pillars of the GCI.

In this essay, Palestine's performance is evaluated in relation to the five GCI pillars, the best practices in cybersecurity are examined, and the GCI questionnaire is reviewed in 2024(5th edition). The following section of the study evaluates Palestine's performance across all GCI pillars

and indicators and identifies any gaps. They therefore serve as a list of actions for the areas that need development, as shown in "Table IV", Assessment of Palestine's performance in the GCI Pillars [13][15][25][26].

TABLE IV. ASSESSMENT OF PALESTINE'S PERFORMANCE IN THE GCI PILLARS

NO	Pillar	Indicators	Performance (GCI 2024)	Assessment (Summary)
1	Legal	• Cybersecurity legislation • Data Protection Regulations • Critical Infrastructure regulations	14.24 / 20.00	Law by Decree No. 10/2018 covers cybercrime but lacks personal-data/privacy protection, breach-notification rules, mandatory audits, and a government-approved framework for international standards, leaving gaps in child protection, privacy and identity-theft deterrence.
2	Technical	• Active CIRTs • Engaged in a regional CIRT • Child Online Protection reporting mechanisms	9.60 / 20.00	A single CERT under the Ministry exists, but there is no national or sectoral framework for global standards, no sectoral CERTs, no international memberships or TI certifications, and no child-protection agency or tools.
3	Organizational	• National Cybersecurity Strategies • Cybersecurity Agencies • Child Online Protection initiatives	2.38 / 20.00	Sectoral IT/telecom strategy and an information-security policy team exist, but there is no overarching national cybersecurity strategy, governance framework, or benchmark standard, nor a dedicated national agency for cybersecurity or child-protection programs.
4	Capacity Development	• Cyber-awareness initiatives • Cybersecurity R&D programs • National cybersecurity industries	9.04 / 20.00	The Ministry runs awareness workshops and bulletins, but there are no national or industry R&D projects, no data on certified public-sector staff, and no certified organizations following international cybersecurity standards.
5	Cooperation	• Public-Private Partnerships • Bilateral agreements • Multilateral agreements	2.46 / 20.00	There is no mechanism for sharing cybersecurity resources with other countries or between public/private sectors, and no known bilateral or multilateral cybersecurity agreements or alliances.

The "Table IV" shows Palestine's status in five pillars of cybersecurity according to the GCI 2024: The legal pillar (14.24/20) indicates that a cybercrime law has been in place since 2018, but it lacks data protection, breach notification, and implementation of international standards; the technical pillar (9.60/20) includes a single CERT under the Ministry's supervision, but without national or sectoral frameworks, international memberships, or child protection mechanisms; the regulatory pillar (2.38/20) includes sectoral and information security strategies, but lacks a national strategy, governance framework, or dedicated agency; the capacity building pillars (9.04/20) are limited to awareness workshops and bulletins, with no research projects or accredited training; and finally, the cooperation pillar (2.46/20) highlights the absence of public/private partnerships or bilateral or multilateral agreements.

V. CONCLUSION AND FUTURE RECOMMENDATIONS

Analysis of the Global Cybersecurity Index (GCI) data for the period 2017–2024 shows a widening gap between Palestine and Saudi Arabia. Palestine saw a slight improvement in the 2018 edition, followed by a gradual decline in ranking and score during the 2020 and 2024 editions, while Saudi Arabia made significant strides, reaching first place with a perfect score in 2024. [15][16][28] This indicates that Palestinian efforts have been intermittent or insufficient to achieve tangible progress compared to leading countries. Furthermore, a comparative legal analysis has shown that the Palestinian Anti-Cybercrime Law (Decree 2018) covers core crimes but lacks significant updates related to data protection, privacy, international cooperation mechanisms, and practical enforcement of judgments. [11] The Saudi framework, on the other hand, has a more integrated legislative system that is regularly updated and links it to other laws and international standards, such as the Budapest Convention on Cybercrime [12][21][22].

A. EVALUATING THE EFFECTIVENESS OF LEGISLATION AND INSTITUTIONS

Qualitative findings and the Palestinian context indicate that the existence of strict legal texts alone is not sufficient. Effective deterrence depends on the ability of judicial and security authorities to investigate and enforce crimes in an environment with adequate technical and human resources and effective international cooperation mechanisms. In Palestine, partial Israeli control over digital infrastructure and a lack of digital forensics resources hinder the effective application of sanctions and the prosecution of cybercrimes, diminishing the theoretical deterrent effect enshrined in the law [11][27]. The Saudi experience highlights how the presence of a strong national body, dedicated resources, and regular capacity-building programs translates legislative text into effective practice, supported by international cooperation agreements and coherent enforcement mechanisms [12][14].

B. STRATEGIC RECOMMENDATIONS OBJECTIVES

Based on integrating the results of the GCI's quantitative analysis with qualitative and contextual analysis, the Palestinian national strategy should focus on updating the legislative framework by issuing or amending legislation to

protect personal data and privacy, detailing mechanisms for reporting cyber incidents, and including provisions for international cooperation based on the Budapest Convention and other international standards [21][22][11]. Technical and organizational capabilities should also be enhanced by establishing or strengthening local digital forensics units and CERT/CIRTs, adopting international standards for accreditation and training, and investing in human resources through internationally recognized programs and certifications [27][28]. This also requires establishing a national cybersecurity authority or higher committee with clear powers to oversee and coordinate between government agencies, the private sector, and universities, with flexibility to address environmental and political constraints. Furthermore, memoranda of understanding and bilateral and regional agreements should be drafted with supporting countries and organizations to enhance investigations and information exchange, taking into account the Palestinian political situation and the constraints of limited international recognition. Finally, performance should be monitored and progress measured by adopting internal indicators derived from the five GCI pillars and preparing periodic reports to analyze progress and address gaps quickly [15][16][28].

C. Implementation Priorities and Approximate Timeline

In the short-term phase (6–12 months), a rapid legislative review will be conducted to include provisions for data protection, reporting mechanisms, and international cooperation. Initial awareness and training workshops will be launched for legal and security personnel on digital forensics and privacy protection. The institutional structure of the National Cybersecurity Authority will be established, with initial powers and responsibilities defined [27].

In the medium-term phase (1–3 years), legislation related to data protection, privacy, e-commerce, and critical infrastructure will be finalized and harmonized with the Cybercrime Law. Specialized digital forensics units will be established, equipped with appropriate tools and training. The first international cooperation agreements will be signed with countries and specialized organizations to support investigations and information exchange. National programs will be launched to build technical capabilities through academic partnerships and advanced courses.

In the long-term phase (3–5 years and beyond), legislation and the institutional framework are periodically evaluated and updated to keep pace with technological developments such as artificial intelligence, cloud computing, and the Internet of Things. International partnerships are expanded, regional cooperation is activated, and cybersecurity is engaged in global initiatives such as ITU programs and joint research projects. Cybersecurity is integrated into national development strategies, while securing continued and sustainable funding and high-level political support. Performance indicators (KPIs) linked to the GCI pillars and the results of stakeholder reviews are assessed at each phase [15][16][28].

D. Constraints and Considerations

The fundamental constraints stem from the geopolitical environment imposed by Israeli control over part of the digital infrastructure. This necessitates the search for alternative solutions, such as partnerships with international providers or initiatives that rely on advanced encryption technologies to preserve digital sovereignty as much as possible [26][27]. Palestine also faces limited resources, requiring efforts to attract international, technical, and financial support from donors and international organizations to cover capacity building and infrastructure development. Limited international recognition may affect the possibility of formally joining some agreements. Therefore, special cooperation formulas can be negotiated, or accession can be achieved through technical presence or through intermediary partners. Flexible mechanisms must also be ensured for the continuous updating of legislation, procedures, and capabilities in light of rapid technological development.

E. Future Trends and Research Priorities

Applied field studies should be conducted to monitor the implementation of legislation and analyze real-life cases of cybercrime in Palestine to assess the effectiveness of legislation and investigative mechanisms in practice [27][24]. It is also advisable to evaluate the impact of interventions after implementing interim recommendations by measuring changes in GCI performance and the actual performance of technical bodies and units, and linking this to periodic reports. Focusing on emerging technologies is of paramount importance, as the future impacts of artificial intelligence, the Internet of Things, and cloud computing on the Palestinian cyber landscape should be studied, and proactive legal and technical frameworks should be developed. Furthermore, it is necessary to strengthen local academic research and encourage multidisciplinary studies that combine law, technology, and public policy, while monitoring international practices and the experiences of countries with similar environments (e.g., emerging countries or those under geopolitical pressure) to draw lessons and continuously update strategies.

REFERENCES

[1] Dr. Niranjan Seshadri, "Understanding the four dimensions of life," Dec. 04, 2019.

[2] J. Stein Schjølberg and A. M. Hubbard, "WSIS Thematic Meeting on Cybersecurity HARMONIZING NATIONAL LEGAL APPROACHES ON CYBERCRIME," Geneva, Jun. 2005.

[3] Cyber Security Agency of Singapore, "The Singapore Cybersecurity Strategy 2021." 2021. [Online]. Available: www.apt811.com

[4] "ITU NATIONAL CYBERSECURITY STRATEGY GUIDE," 2011. [Online]. Available: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf

[5] Prof. Dr. Marco Gercke, "Understanding cybercrime: Phenomena, challenges and legal response," Nov. 2014. [Online]. Available: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

[6] Shane Cross INTERPOL, Simon Hirrle INTERPOL, May-Ann Pte Ltd, and Lim-TRPC Pte Ltd, "National Cybercrime Strategy Guidebook," 2021.

[7] Council of Europe, "The Budapest Convention on Cybercrime: benefits and impact in practice," Strasbourg, Jul. 2020. [Online]. Available: www.coe.int/cybercrime

[8] S. Schjolberg, "The History of Global Harmonization on Cybercrime Legislation-The Road to Geneva," 2008. [Online]. Available: www.cybercrimelaw.net.

[9] International Telecommunication Union, "Cybersecurity guide for developing countries," 2007. [Online]. Available: www.itu.int/ITU-D/e-strategies

[10] BDT, Pol, and CYB, "ITU Publication on Understanding Cybercrime: A Guide for Developing Countries," 2009.

[11] "Law by Decree No. 10 of 2018 on Cybercrime," 2018.

[12] "Anti-Cyber Crime Law Translation of Saudi Laws," 2007.

[13] ITU, "Global Cybersecurity Index 2020 Measuring commitment to cybersecurity Acknowledgements," 2020.

[14] GOV. S. Unified National Platform, "Cybersecurity in the Kingdom," 2021.

[15] ITU, "Global Cybersecurity Index (GCI) 2017 ITU-D," 2017.

[16] Itu, "Global Cybersecurity Index (GCI) 2018 ITUPublications Studies & research."

[17] N. & U. S. G. A. R. IGO, "International and Foreign Cyberspace Law Research Guide," Mar. 21, 2021. International and Foreign Cyberspace Law Research Guide (accessed Nov. 30, 2021).

[18] ITIC, "Organizations and Institutions that Address International Cybersecurity," Organizations and Institutions that Address International Cybersecurity, 2021. 5. https://www.itic.org/dotAsset/c/c/cc91d83a-e8a9-40ac-8d75-0f544ba41a71.pdf (accessed Nov. 30, 2021).

[19] Thomson Reuters and Institute of Electrical and Electronics Engineers, 8th IEEE International Conference, Application of Information and Communication Technologies - AICT 2014 : conference proceedings : 15-17 October 2014, Astana, Kazakhstan. 2015.

[20] P. Gottschalk, Policing cyber crime. BookBoon, 2010.

[21] "European Treaty Series - No. 185," Budapes, Dec. 2001. Accessed: Dec. 01, 2021. [Online]. Available: https://rm.coe.int/1680081561

[22] Council of Europe, "The budapest convention," 2021. https://www.coe.int/en/web/cybercrime/the-budapest-convention (accessed Dec. 01, 2021).

[23] A. Alabdulatif, "CYBERCRIME AND ANALYSIS OF LAWS IN KINGDOME OF SAUDI ARABIA," 2018.

[24] "Cybercrime Convention Committee" (T-CY), "Mapping study on cyberviolence," Jul. 2018. [Online]. Available: www.coe.int/cybercrime

[25] UNIDIR, "Saudi Arabia CYBERSECURITY POLICY Strategy Documents National Cybersecurity Strategy (NCS) National Cybersecurity Authority (NCA) Implementation Frameworks The National Cryptographic Standards (NCS) National Cybersecurity Authority (NCA)," Mar. 2021.

[26] United Nations Statistics Division, "CYBERWELLNESS PROFILE STATE OF PALESTINE BACKGROUND Total Population: unknown," 2015. [Online]. Available: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx

[27] Ministry of Telecom & Information Technology State of Palestine, "Sectoral strategic plan for telecommunications, information technology, and post 2017-2022," Sectoral strategic plan for telecommunications, information technology, and post 2017-2022, Nov. 2016. https://www.mtit.pna.ps/Content/files/plains_and_strategies/en/-8586172493377581909Strategic%20Plan%202017-2022.pdf (accessed Nov. 30, 2021).

[28] International Telecommunication Union, Global Cybersecurity Index (GCI) 2024, 5th ed., Geneva, Switzerland: ITU, 2024. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[29] Creswell, J. W., & Plano Clark, V. L. (2018). Designing and Conducting Mixed Methods Research (3rd ed.). Thousand Oaks, CA: SAGE.