Cybercrime in Egypt: Evolving Threats, Legal Responses, and Future Challenges

Mohamed S. Sagawy[1*], Khaled A. Muhammad[2], Ahmed T. Hussein[1] and Muhammad M. Al-Mardani[3]

[1] Environmental Legalization Sciences Department, Institute of Environmental Studies, Arish University, North Sinai, 45516, Egypt
[2]Department of Sociology, Faculty of Arts, Arish University, North Sinai, 45516, Egypt.
[3]Faculty of Education, Arish University, North Sinai, 45516, Egypt.

Abstract:
This paper investigates the changing nature of cybercrime in Egypt and evaluates the legislative and institutional measures taken by the government to address this increasing menace. Utilizing contemporary laws, policy papers, and academic literature, the research investigates the characteristics and extent of cyber threats Egypt is experiencing. It assesses the efficacy of existing countermeasures and highlights areas that require enhancement. The study employs a qualitative method that combines document analysis, literature review, and case study investigation. It aims to answer four important questions about cybercrime patterns, the growth of the legal environment, present issues, and prospective improvements to Egypt's cybersecurity capabilities. The findings indicate a threefold rise in reported cybersecurity events from 2018 to 2021. The most common incidents include financial fraud, identity theft, ransomware attacks, and cyber espionage. Egypt has formulated extensive legislative frameworks and formed crucial institutional institutions as a reaction. Nevertheless, there are ongoing difficulties in terms of the ability to enforce laws, the level of knowledge and skills in using digital technology, finding a balance between security and individual rights, prosecuting crimes that occur across national borders, including private companies in addressing these issues and addressing gaps in technology. The study suggests several areas for improvement, such as enhancing the training and resources available to law enforcement, fostering collaboration between public and private sectors, strengthening cooperation between countries, promoting digital literacy, refining laws, improving the protection of critical infrastructure, and increasing investment in cybersecurity research and development. Although Egypt has made notable progress in establishing its cybersecurity framework, the ever-changing nature of cyber threats requires continuous monitoring, adaptability, and innovation. Potential areas for future study might encompass conducting empirical investigations into targeted preventative strategies, conducting comparative assessments of regional forms of cybersecurity governance, and exploring the potential of new technology to bolster cyber defence capabilities.

Keywords: Cybercrime, Egypt, Cybersecurity law, Digital Transformation, Information technology crimes

1. Introduction:

The swift and widespread adoption of information and communication technology has brought us a period of unparalleled digital interconnectedness and creativity. Nevertheless, the advent of the digital revolution has also spawned novel types of criminal behavior that capitalize on the weaknesses of interconnected systems and networks (Wall, 2024). Cybercrime has become a significant danger to individuals, corporations, and national security, going beyond geographical limits and posing challenges to conventional law enforcement methods (Atrey, 2023, Shah, 2024, Broadhurst et al., 2014).

In recent years, Egypt, similar to several developing nations, has witnessed a significant increase in the use of Internet services and the implementation of digital transformation projects. In 2021, the total number of individuals using the internet in Egypt amounted to 57.3 million, which accounts for around 55% of the country's population (Elgohary, 2022). Although the expansion of digital technology has provided many advantages in terms of social and economic development, it has also made the country more vulnerable to increased cybersecurity threats (Saeed et al., 2023). The Egyptian government has documented a significant surge in many types of cybercrime, including financial fraud, identity theft, and attacks on critical infrastructure (Allen et al., 2024).

Egypt has implemented substantial measures to enhance its legal and institutional framework to tackle cybercrime, as stated by Van Vuuren et al. (2019). Implementing the Anti-Cyber and Information Technology Crimes Law in 2018 was significant in the nation's endeavors to combat digital dangers. Nevertheless, the efficacy of these measures and their consequences for civil liberties and digital rights have been topics of continuous discussion (Hassib and Alnemr, 2021).

This research aims to conduct a thorough analysis of the cybercrime situation in Egypt. This analysis will involve studying the characteristics of cyber threats, assessing the effectiveness of the country's legislative and policy measures, and identifying significant obstacles and potential areas for enhancement. This endeavor aims to provide a valuable addition to the existing literature on cybersecurity governance in underdeveloped nations. Furthermore, it aims to provide valuable insights that might guide policy formulation in Egypt and other comparable settings. The research seeks to answer the following fundamental inquiries: (i) What are the main manifestations and patterns of cybercrime impacting Egypt? (ii) What changes have occurred in Egypt's legislative and institutional framework for addressing cybercrime in recent years? What are the primary obstacles and constraints in Egypt's present strategy for preventing and responding to cybercrime? Furthermore, how can Egypt improve its cybersecurity skills and promote international collaboration in this field?

2. Materials and Methods:

This study employs a qualitative approach, combining document analysis, literature review, and case study examination. The following methods were utilized to gather and analyze data:

2.1. Legal and Policy Document Analysis:

A comprehensive review of Egyptian legislation related to cybercrime was conducted, focusing on critical laws such as:

a. Law No. 175 of 2018 on Anti-Cyber and Information Technology Crimes
b. Law No. 151 of 2020 on Personal Data Protection
c. Telecommunications Regulation Law No. 10 of 2003

Additionally, policy documents, strategy papers, and official reports from relevant government agencies, including those from the Ministry of Communications and Information Technology (MCIT) and the National Telecom Regulatory Authority (NTRA), were examined.

2. 2. Literature Review

An extensive academic literature review, reports from international organizations, and cybersecurity industry publications was conducted. This review covered Egypt-specific studies and broader research on cybercrime trends and governance in developing countries. Databases such as Google Scholar, JSTOR, and IEEE Xplore were utilized to identify relevant peer-reviewed articles and conference papers.

2.3. Comparative Analysis

Egypt's cybercrime legislation and policies were compared with those of other countries in the Middle East and North Africa (MENA) region and with international best practices to identify strengths, weaknesses, and potential areas for improvement.

2.4. Data Analysis

The collected data was analyzed using thematic content analysis. Key themes and patterns were identified across the various sources, with particular attention paid to (i) evolving cybercrime trends and tactics, (ii) legislative and policy developments, (iii) institutional capacity and coordination, (iv) challenges in enforcement and prosecution, (v) international cooperation initiatives, and (vi) balancing security needs with civil liberties. The analysis aimed to synthesize findings from multiple sources to provide a comprehensive picture of Egypt's cybercrime landscape and governance approach.

2.5. Limitations

It is important to note certain limitations of this study. The sensitive nature of cybersecurity issues means that some information, particularly regarding specific incidents or government capabilities, may not be publicly available. Additionally, the rapidly evolving nature of cybercrime and related policies means that some information may become outdated quickly. Efforts were made to use the most recent available data and to cross-verify information from multiple sources where possible.

3. Results and Discussion

3.1. Cybercrime Landscape in Egypt

Egypt has witnessed a significant increase in cybercrime activities in recent years, mirroring global trends and reflecting unique local challenges. According to the Egyptian Computer Emergency Response Team (EG-CERT), the number of reported cybersecurity incidents increased by 300% between 2018 and 2021 (Voronenko et al., 2022). The most prevalent forms of cybercrime in Egypt include:

3.1.1. Financial Fraud

Online banking fraud, credit card theft, and phishing attacks targeting financial institutions have become increasingly sophisticated. In 2020, the Central Bank of Egypt reported a 20% increase in

attempted cyber attacks on banking systems compared to the previous year (CBE, 2021). A notable case involved a coordinated attack on multiple ATMs in Cairo, resulting in the theft of approximately 2 million Egyptian pounds (Neagu and Savu, 2019).

3.1.2. Social Engineering and Identity Theft

Cybercriminals have exploited the growing use of social media platforms to conduct social engineering attacks and identity theft. The Egyptian Ministry of Interior reported over 5,000 cases of online identity theft in 2021, with many victims experiencing financial losses or reputational damage (Michail, 2022).

3.1.3. Ransomware and Malware

Egyptian businesses and government agencies have faced increasing threats from ransomware attacks. In 2019, a significant ransomware attack targeted several government websites, temporarily disrupting services and highlighting vulnerabilities in the country's digital infrastructure (Horak, 2023).

3.1.4. Cyber Espionage

While less publicly discussed, cyber espionage targeting government institutions and strategic industries remains a significant concern. Egyptian authorities have reported attempts by foreign state-sponsored actors to infiltrate critical infrastructure systems, though specific details are often not disclosed for security reasons (NTRA, 2020).

3.1.5. Online Extremism and Disinformation

The use of social media and messaging platforms to spread extremist ideologies and disinformation has been identified as a growing threat to national security and social stability. Egyptian authorities have cited this as a justification for increased online surveillance and content regulation measures (Hassib and Shires, 2021). These trends highlight Egypt's diverse and evolving cyber threats, necessitating a comprehensive and adaptive approach to cybersecurity governance.

3.2. Legal and Institutional Framework

Egypt has made significant strides in developing its legal and institutional framework for combating cybercrime in recent years. Key developments include:

3.2.1. Anti-Cyber and Information Technology Crimes Law (Law No. 175 of 2018)

This landmark legislation provides a comprehensive legal framework for addressing various forms of cybercrime. It criminalizes a wide range of online activities, including unauthorized access to information systems, data theft, and the spread of extremist ideologies through digital platforms. The law also empowers law enforcement agencies to block websites deemed to pose a threat to national security or public morals (ARE, 2018).

3.2.2. Personal Data Protection Law (Law No. 151 of 2020)

Recognizing the importance of data protection in the digital age, this law establishes rules for public and private entities to collect, process, and store personal data. It also creates a dedicated

regulatory body, the Center for Personal Data Protection, to oversee compliance and handle complaints (AlAshry, 2022).

3.2.3. Establishment of the Supreme Council for Cyber Security
Created by presidential decree in 2014, this high-level body is responsible for formulating national cybersecurity strategies and coordinating efforts across government agencies (Hassib and Alnemr, 2021).

3.2.4. National Cybersecurity Strategy
Launched in 2017, this strategy outlines Egypt's vision and objectives for enhancing its cybersecurity capabilities, focusing on critical infrastructure protection, capacity building, and international cooperation (Allen et al., 2024).

3.2.5. Egyptian Computer Emergency Response Team (EG-CERT)
Established under the National Telecom Regulatory Authority, EG-CERT plays a crucial role in monitoring cyber threats, coordinating incident response, and providing technical support to government agencies and critical infrastructure operators (NTRA, 2020). These legislative and institutional developments demonstrate Egypt's commitment to addressing cybersecurity challenges. However, their implementation and effectiveness have faced several challenges, which will be discussed in the following section.

3.3. Challenges and Limitations
Despite the progress made in developing a legal and institutional framework for cybersecurity, Egypt faces several challenges in effectively combating cybercrime:

3.3.1. Enforcement Capacity
Law enforcement agencies and the judiciary often lack the technical expertise and resources to investigate and prosecute complex cybercrime cases effectively. This has resulted in a low conviction rate for cybercrimes, potentially undermining the deterrent effect of legislation (Mphatheni and Maluleke, 2022).

3.3.2. Digital Literacy and Public Awareness
A significant portion of the Egyptian population lacks basic digital literacy skills, making them vulnerable to various forms of online fraud and manipulation. Public awareness campaigns about cybersecurity best practices have been limited in reach and effectiveness (Ahmed Hussien Khalaf, 2022).

3.3.3. Balancing Security and Civil Liberties
The broad powers granted to authorities under the Anti-Cyber and Information Technology Crimes Law have raised concerns about potential infringement on freedom of expression and privacy rights. Human rights organizations have criticized the law's vague language and use to target political dissent (Zayed, 2023).

3.3.4. Cross-Border Challenges

The transnational nature of cybercrime poses significant challenges for Egyptian law enforcement, particularly in cases involving foreign-based perpetrators or digital evidence stored in other jurisdictions. Egypt's participation in international cybercrime cooperation frameworks remains limited (Alramamneh and Abuanzeh, 2023).

3.3.5. Private Sector Engagement

While the government has taken steps to enhance cybersecurity in critical infrastructure sectors, engagement with the broader private sector on cybersecurity issues remains inadequate. Many small and medium-sized enterprises lack the resources and expertise to implement robust cybersecurity measures (Elbarky and Elgamal, 2023).

3.3.6. Technological Gaps

Egypt's cybersecurity capabilities lag behind those of more technologically advanced nations, particularly in artificial intelligence-driven threat detection and quantum-resistant cryptography. This technological gap may leave the country vulnerable to sophisticated cyber attacks (Abd El-Latif et al., 2023).

3.4. Opportunities for Improvement

Addressing the challenges outlined above requires a multifaceted approach. Several opportunities for enhancing Egypt's cybercrime prevention and response capabilities include:

3.4.1. Capacity Building and Specialization

Investing in specialized training programs for law enforcement officers, prosecutors, and judges to enhance their technical skills in handling cybercrime cases. Establishing dedicated cybercrime units within the police force and prosecution services could improve the effectiveness of investigations and prosecutions (Brown, 2015).

3.4.2. Public-Private Partnerships

Fostering closer collaboration between government agencies, private sector companies, and academic institutions to share threat intelligence, develop cybersecurity solutions, and promote best practices. The establishment of a national cybersecurity innovation hub could facilitate such partnerships (Tropina et al., 2015).

3.4.3. International Cooperation

Strengthening Egypt's participation in international cybercrime cooperation frameworks, such as the Budapest Convention on Cybercrime, to enhance cross-border investigation capabilities and information sharing. Developing bilateral cybersecurity agreements with key partner countries could also bolster Egypt's cyber defences (Hassib and Alnemr, 2021).

3.4.4. Enhancing Digital Literacy
Integrating cybersecurity education into school curricula and launching comprehensive public awareness campaigns to improve digital literacy and promote safe online behaviors across all segments of society (Kont, 2023).

3.4.5. Refining Legal Frameworks
Regularly reviewing and updating cybercrime legislation to address emerging threats and technologies while ensuring that legal provisions balance security needs and civil liberties appropriately. Establishing more precise guidelines for the implementation of cybercrime laws could help address concerns about potential misuse (Salim and Dhafri, 2024).

3.4.6. Critical Infrastructure Protection
Developing sector-specific cybersecurity standards and requiring regular security audits for critical infrastructure operators. Implementing advanced threat detection and response systems across critical sectors could enhance resilience against sophisticated cyber attacks (NTRA, 2020).

3.4.7. Research and Development
Increasing investment in cybersecurity research and development, focusing on emerging technologies such as artificial intelligence, blockchain, and quantum computing. Establishing research partnerships with leading international institutions could help bridge technological gaps (Abd El-Latif et al., 2023).

4. Conclusion
Egypt's efforts to combat cybercrime have made significant progress in recent years, particularly in developing a comprehensive legal framework and establishing critical institutional structures. The Anti-Cyber and Information Technology Crimes Law of 2018 and the Personal Data Protection Law of 2020 represent important milestones in the country's cybersecurity governance. However, the rapidly evolving nature of cyber threats and challenges in enforcement capacity, digital literacy, and international cooperation underscore the need for continued adaptation and improvement. Egypt must adopt a holistic approach beyond legislative measures to effectively address the multifaceted challenges of cybercrime. This approach should prioritize capacity building across law enforcement and judicial institutions, foster closer collaboration between the public and private sectors, and promote digital literacy and cybersecurity awareness among the general population. Additionally, enhancing international cooperation and investing in cutting-edge cybersecurity technologies will be crucial for staying ahead of increasingly sophisticated cyber threats. As Egypt continues its digital transformation journey, balancing the imperatives of national security and economic development with the protection of civil liberties and digital rights will remain a critical challenge. Transparent and inclusive policymaking processes and regular review and refinement of cybersecurity strategies will be essential for navigating this complex landscape. Future research directions could include empirical studies on the effectiveness of specific cybercrime prevention measures in the Egyptian context, comparative analyses of cybersecurity governance models across the MENA region, and explorations of the potential applications of emerging technologies in enhancing cyber defence capabilities. In conclusion,

while Egypt has made commendable progress in developing its cybersecurity framework, the dynamic nature of cyber threats necessitates ongoing vigilance, adaptation, and innovation. By addressing current challenges and capitalizing on opportunities for improvement, Egypt can strengthen its resilience against cybercrime and position itself as a leader in cybersecurity governance among developing nations.

5. References

ABD EL-LATIF, A. A., MALEH, Y., MAZURCZYK, W., ELAFFENDI, M. & ALKANHAL, M. I. 2023. *Advances in Cybersecurity, Cybercrimes, and Smart Emerging Technologies*, Springer.

AHMED HUSSIEN KHALAF, M. 2022. E-learning environment in Egypt. *International Journal of Education and Learning Research,* 5**,** 116-144.

ALASHRY, M.-S. 2022. Investigating the efficacy of the Egyptian data protection law on media freedom: Journalists' perceptions. *Communication & Society,* 35**,** 101-118.

ALLEN, N., HASHEM, S. & KOLADE, E. 2024. 'Leapfrogging 'lagging'?: highlighting critical information infrastructure protection challenges and opportunities in Egypt and Nigeria. *Journal of Cyber Policy***,** 1-21.

ALRAMAMNEH, I. M. & ABUANZEH, A. 2023. International and National Procedural Framework for Combating Cybercrime. *International Journal of Cyber Criminology,* 17**,** 330–349-330–349.

ARE 2018. Arab Republic of Egypt. "Law No. 175 of 2018 on Anti-Cyber and Information TechnologyCrimes." https://drive.google.com/file/d/1ra7NlKn7Uh_YU5fL7NBKt18JE2mKAKm8/view, access on 22/10/2023.

ATREY, I. 2023. Cybercrime and its Legal Implications: Analysing the challenges and Legal frameworks surrounding Cybercrime, including issues related to Jurisdiction, Privacy, and Digital Evidence. *International Journal of Research and Analytical Reviews*.

BROADHURST, R., GRABOSKY, P., ALAZAB, M., BOUHOURS, B. & CHON, S. 2014. An analysis of the nature of groups engaged in cyber crime. *An analysis of the nature of groups engaged in cyber crime, International Journal of Cyber Criminology,* 8**,** 1-20.

BROWN, C. S. 2015. Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology,* 9**,** 55.

CBE 2021. Central Bank of Egypt. Financial Stability Report 2021. Cairo: CBE. Available at: https://www.cbe.org.eg/en/pages/publications.aspx, Access on 12/12/2023.

ELBARKY, S. & ELGAMAL, S. 2023. An ISM approach for the barrier analysis in implementing Industry 4.0 practices: Egyptian enterprises. *International Journal of Integrated Supply Management,* 16**,** 337-364.

ELGOHARY, E. 2022. The role of digital transformation in sustainable development in Egypt. *The International Journal of Informatics, Media and Communication Technology,* 4**,** 71-106.

HASSIB, B. & ALNEMR, N. 2021. Securitizing cyberspace in Egypt: The dilemma of cybersecurity and democracy. *Routledge Companion to Global Cyber-Security Strategy.* Routledge.

HASSIB, B. & SHIRES, J. 2021. Manipulating uncertainty: Cybersecurity politics in Egypt. *Journal of Cybersecurity,* 7**,** tyaa026.

HORAK, G. 2023. *Personal Details Exposed: Spyware and Human Rights in the Middle East and North Africa.* Harvard University.

KONT, K.-R. 2023. Cyber Literacy Skills of Estonians: Activities and Policies For Encouraging Knowledge-Based Cyber Security Attitudes. *Information & Media*, 80-94.

MICHAIL, M. 2022. The legal protection of Egyptian antiquities in light of digital transformation. *Journal of Law and Emerging Technologies,* 2, 13-52.

MPHATHENI, M. R. & MALULEKE, W. 2022. Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. *International Journal of Research in Business and Social Science (2147-4478),* 11, 384-396.

NEAGU, F. S. & SAVU, A. The costs of cyberterrorism for the national economy: United States of America vs Egypt. Proceedings of the International Conference on Business Excellence, 2019. 983-993.

NTRA 2020. National Telecom Regulatory Authority. Annual Cybersecurity Report 2019-2020. Cairo: NTRA. Available at: https://www.tra.gov.eg/en/reports/.

SAEED, S., ALTAMIMI, S. A., ALKAYYAL, N. A., ALSHEHRI, E. & ALABBAD, D. A. 2023. Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors,* 23, 6666.

SALIM, I. F. & DHAFRI, M. R. 2024. The Criminal Agreement in Cybercrimes in Iraqi, Emirati, and Qatari Law. *Kurdish Studies,* 12, 4060-4087.

SHAH, A. 2024. CYBERCRIME CHRONICLES: EXPLORING THE EVOLVING LANDSCAPE OF CHALLENGES IN THE DIGITAL ERA.

TROPINA, T., CALLANAN, C. & TROPINA, T. 2015. Public–private collaboration: Cybercrime, cybersecurity and national security. *Self-and co-regulation in Cybercrime, cybersecurity and national security*, 1-41.

VAN VUUREN, J., LEENEN, L., PIETERSE, P. & POLICE, S. A. Framework for the Development and Implementation of a Cybercrime Strategy in Africa. Proceedings of the ICCWS 2019 14th International Conference on Cyber Warfare and Security, edited by N. Van Der Waag-Cowling and L. Leenen, 2019. 156-167.

VORONENKO, I., NEHREY, M., LAPTIEVA, A., BABENKO, V. & ROHOZA, K. 2022. National cybersecurity: assessment, risks and trends. *International Journal of Embedded Systems,* 15, 226-238.

WALL, D. S. 2024. *Cybercrime: The transformation of crime in the information age*, John Wiley & Sons.

ZAYED, H. 2023. *Hiding in Plain Sight: How Egyptian Nonprofit Organizations Adapt to Shrinking Civic Space*, American University.