Cyber Threats and Legal Gaps: A Study on Egypt and UAE Laws

Dr. Doaa Mohsen Othman
PhD in Criminal Law
Certified Lecturer at the Judicial Academy - Abu Dhabi

Abstract

This study examines the effectiveness of cybercrime legislation in Egypt and the United Arab Emirates (UAE), two countries facing rising digital threats in a rapidly evolving technological environment. It highlights the growing scale and complexity of cyber threats—including hacking, online fraud, and data breaches—and assesses how each country's legal system responds. the research identifies strengths, overlaps, and critical legal gaps. While both countries have taken significant steps to criminalize various forms of cybercrime, challenges remain in enforcement, international cooperation, and protection of digital rights. The research concludes with targeted recommendations for closing legal loopholes, improving cross-border frameworks, and enhancing institutional capacity to manage cyber risks effectively.

The research also draws on selected international cybercrime cases to highlight the need for harmonized laws and transnational cooperation. this research seeks to provide insights into how Egypt and the UAE can strengthen their cybercrime legislation and enhance cybersecurity resilience.

Cybercrime refers to criminal activities that are carried out using computers or the internet, including offenses such as hacking, identity theft, online fraud, data breaches, and cyberterrorism. With the increasing digitization of personal, financial, and government systems, cybercrime has become a

(ISSN: 2537 - 0758)

global threat affecting individuals, corporations, and states alike.

In the Middle East, both Egypt and the United Arab Emirates (UAE) have experienced rapid digital growth, making them vulnerable to sophisticated cyber threats. In response, Egypt introduced Law No. 175 of 2018 on combating information technology crimes, while the UAE enacted Federal Decree-Law No. 34 of 2021 to address cybercrime and misinformation. Despite these developments, the pace and complexity of cyber threats continue to outstrip the existing legal responses.

This research addresses the core problem of whether the current cybercrime laws in Egypt and the UAE adequately respond to modern cyber threats. It investigates if there is a mismatch between legislative intent and practical enforcement, and whether the laws are flexible enough to adapt to rapidly changing digital risks.

The main objectives of this study are:

• To examine the current legal frameworks in Egypt and the UAE related to cybercrime

• To identify gaps and limitations in existing laws

• To evaluate enforcement mechanisms and institutional capacities

• To provide recommendations for legal and policy reform

Keywords: Cybercrime, Egypt, United Arab Emirates, Cybersecurity Law, Digital Threats, Legal Frameworks, Enforcement Challenges, Data Protection, Comparative Legal Analysis.

Research methodology

This study adopts a comparative legal analysis methodology, focusing on the content of cybercrime laws, their application, and alignment with international standards.

1 Introduction

The Internet, a global system of interconnected computer networks, is one of the most defining technologies of our time. Most aspects of our lives are touched in some form or another by the Internet, including our economic and financial systems, our social interactions, our education, work and civic participation, as well as the many services we use to complement our lives, from entertainment and banking services to booking travel. In many ways, the Internet has become an indispensable aspect of modern life – and peoples' dependence on the Internet and its ecosystem of services will only continue to grow.

The central idea is that the rise and severity of aggressive communication in online networks can be traced back to the nature of communication culture within those networks. Thompson's categorization of communication types in his 1995 work "The Media and Modernity" offers insight. He identifies three types, Face-to-face interaction – happens in the same time and space, using rich symbolic cues (tone, body language). Mediated interaction – such as phone calls or emails, reduces these cues but still allows for dialogue. Mediated quasi-interaction – such as newspapers or traditional TV, targets a general audience rather than specific individuals, making it more monologic (one-way communication).

The key distinction is that while face-to-face and mediated interaction are dialogic (two-way), mediated quasi-interaction is monologic (one-way), which may contribute to the way aggressive communication spreads online ([1]).

Briefly will explain how the Internet works, how information travels over the Internet, and how the Internet is governed.

[1] Die strafrechtliche Verantwortlichkeit von Anbietern (innerhalb) sozialer Netzwerke, Maximilian Nussbaum, Published by: Duncker & Humblot GmbH. (2025), P.70,

(ISSN: 2537 - 0758)

Internet Governance Tools

The Internet is managed using tools like: **Laws and policies** (set mostly by governments, e.g., for 5G rollout), **Technical standards** (set by groups like ICANN for domain names and IETF for network compatibility), **Codes of conduct** (developed by private companies for app usage), **Content regulation** (e.g., censorship laws in certain countries like China).

Layers of the Internet([2])

1. **Infrastructure Layer**: The physical hardware that carries data—like computers, cables, satellites, and wireless systems
2. **Logical Layer**: The rules and systems that guide data through the infrastructure—like the DNS which connects domain names to IP addresses.
3. **Applications Layer**: The software we use to access the Internet—such as browsers, email apps, and online games.
4. **Content Layer**: The actual information online—text, images, videos, podcasts, etc. So, the Internet functions like a digital postal system, with different layers handling the transport, direction, tools, and messages—while various actors (governments, companies, nonprofits) govern and coordinate how everything runs.

Recent data shows a sharp rise in cyberattacks over the past decade, with increasingly sophisticated and harmful methods. According to Check Point Research, as of May 2021, there was a 70% year-on-year increase in weekly cyberattacks on U.S. organizations and a 97% increase in the EMEA region. This surge highlights the growing scale and complexity of cyber threats. Among the most significant risks are

[2] Internet Governance: Past, Present and Future by Wade Hoxtell and David Nonhoff, Global Public Policy Institute (GPPI), Konrad Adenauer stiftung, P.6

ransomware attacks, supply-chain breaches, and the rise of cybercrime as a service (CaaS), all of which pose serious challenges to global cybersecurity([3]).

2 Define cybercrime and its global impact

In the age of ICT, cybercrime is a relatively new phrase. ICT is useful in all knowledge-and service-based industries. Simply described, cybercrime is defined as crime done through the use of technological devices and related technologies. Technology use has many advantages, but when technology is misused in society, it is illegal. Different types of cybercrimes, such as fraud, hacking, cyberwarfare, cyberstalking, and cyberbullying, are harming intellectual pursuits and causing social problems for society as a whole([4]).

Following the introduction of "computer crime," researchers have formulated additional terminology to categorize related illicit activities. These terms and their corresponding definitions include ([5]):

Digital crime: Any criminal activity involving computers, networks, or other digital devices.

Electronic crime: An illegal act carried out using a computer or electronic media.

Internet crime: Any illegal activity involving components of the Internet, such as websites, chat rooms, or email. This often involves using the Internet to communicate false or fraudulent

[3] PROFESSIONAL ARTICLE: CYBERSECURITY PRIVATE-PUBLIC PARTNERSHIPS: A BRIDGE TO ADVANCE GLOBAL CYBERSECURITY, Ben Haklai ,56 Tex. Tech L. Rev. 627, Spring, 2024, P.7,

[4] Cyber Security, Cyber Crime and Measures to Prevent in Libraries, Mr. Gulshan Kumar Sachdeva & Mr. Muksesh Sachdeva, CPJ Law Journal, Volume XVII Jan 2025,

[5] The Palgrave Handbook of International Cybercrime and Cyber deviance, Defining Cybercrime, P.9, BrianK.Payne, June 2020

(ISSN: 2537 - 0758)

information and includes schemes like advance-fee scams, non-delivery of goods, hacking, and fake employment opportunities.

Network crime: This encompasses not only data interception, but also unauthorized network intrusion to access, change, or destroy data, or to use network resources without permission.

Techno crime: A broad term referring to crimes committed within the technological system.

Virtual crime: Crimes committed in virtual reality settings or virtual games.

A special criminogenic factor is the use of new tools like social bots to spread aggressive communication. When users deploy bots disguised as real people to share or create hostile content, this is no longer spontaneous aggression, these bots become strategic tools used to manipulate the communication environment. This can lead to a distorted perception of public opinion, further amplified by algorithm-driven content curation ([6]).

3 Cybercrime Development: Practical Applications and Cases

Cybercrimes and hacking have been part of the digital world since the earliest days of computers. From the first major hacks in the 1970s, when phone phreakers like John Draper exploited telephone networks, to today's global cyberattacks targeting corporations and governments, the methods and impact of cybercrime have constantly evolved. Early hackers were often driven by curiosity or a desire for recognition, but over time, cybercrime has become a major threat fueled by financial gain, political motives, and even warfare. Understanding the history of these attacks helps reveal how

[6] Die strafrechtliche Verantwortlichkeit von Anbietern (innerhalb) sozialer Netzwerke, Maximilian Nussbaum, Published by: Duncker & Humblot GmbH. (2025), P.80

technology's growth has created both incredible opportunities and serious vulnerabilities. Remembered as one of the most notorious hackers in internet history, Kevin Mitnick started out with a humble interest in ham radio and computing. From the 1970s until 1995 Mitnick penetrated some of the most highly-guarded networks in the world, including those of Motorola and Nokia. Mitnick used elaborate social engineering schemes, tricking insiders into handing over codes and passwords and using the codes to access internal computer systems. He was driven by a desire to learn how such systems worked, but became the most wanted cyber-criminal of the time. Mitnick was jailed twice, in 1988 and 1995, and was placed in solitary confinement while in custody, for fear that any access to a phone could lead to nuclear war.

While some hackers and viruses are remembered for the unusual or funny, a malicious computer virus, first discovered in 2010, will go down in history for a very different reason. The Stuxnet worm has been called the world’s first digital weapon. Unlike other viruses, the worm seems to have been designed to cause physical damage to equipment controlled by computers. It was the first known case of hackers being able to elicit physical damage on real-world equipment, making it very complex and rather frightening. The worm was designed to target control systems used to monitor industrial facilities and was first discovered in nuclear power plants in Iran after a large number of uranium centrifuges began breaking unexpectedly. The worm, for which no one claimed responsibility, knocked out approximately one-fifth of the enrichment centrifuges used in Iran’s nuclear programme,

(ISSN: 2537 - 0758)

damage which is estimated to have put the programme back by as much as two years ([7]).

The role and behavior of states has been rapidly evolving in the field of cybersecurity, as states have assumed much greater roles in promoting cybersecurity among their citizens as well as corporate and other entities within their borders. At the same time, many states are calling attention to other states as potential threats to cybersecurity. For example, the 2021 Microsoft Exchange attacks involved a series of sophisticated data breaches which the United States (US), United Kingdom (UK), European Union (EU), the Northern Atlantic Treaty Organization (NATO) and several other countries attributed to a hacking group publicly alleged to have ties to China's Ministry of State Security. This was the first time that multiple governments and international governmental organizations collectively sought to hold one state responsible for such behavior (US White House 2021), with other countries such as Australia also releasing their own statements expressing concern over China's malicious cyber activity. State (mis)behavior has now become an overt topic in many cybersecurity strategies across the Global North. For example, the EU's most recent cybersecurity strategy includes a statement on "advancing responsible state behavior in cyberspace", aligned to a larger ideal of a global, open, stable and secure internet where international law is respected. From a criminological perspective, the question of state behavior has been approached in a national security context, with areas of concern including potential attacks on critical infrastructure, theft of intellectual property, trade secrets and so on. Much less considered has been the role of states in the context of other cybercrimes, particularly financially

[7] Hacking through history, Jade Fell, Engineering & Technology (Volume: 12, Issue: 3, April 2017), P.30

motivated crime, which reveal complex relationships between states and cyber criminals. Nowhere is this complexity more apparent than in the area of ransomware ([8]).

On December 24, 2024, the United Nations General Assembly adopted the Cybercrime Convention, marking the first international criminal justice treaty of the 21st century. While the Convention has been widely welcomed as a significant step toward global cooperation in combating cyber-enabled crime, several states, including the United States, expressed cautious optimism regarding its effectiveness. The United States emphasized that the Convention—when implemented alongside strong domestic legal safeguards—has the potential to enhance the international community's capacity to address the evolving and pervasive threats posed by cybercrime, including ransomware attacks, cyber-enabled financial fraud, and unlawful intrusions into computer systems and networks.

Nevertheless, the Convention falls short in addressing the gendered dimensions of cybercrime, despite the fact that many forms of digital crime—such as online sexual exploitation, cyber harassment, and trafficking for sexual purposes—disproportionately affect women and girls. This omission is particularly striking when compared to the language of earlier United Nations instruments, such as the General Assembly Resolution from its seventy-fifth session, which highlighted the "feminization of poverty" as a risk factor contributing to the vulnerability of women and girls to trafficking and exploitation. While the Cybercrime Convention includes general references to protecting vulnerable groups, it stops short of explicitly acknowledging gender-based violence in

[8] RANSOMWARE THROUGH THE LENS OF STATE CRIME: CONCEPTUALIZING RANSOMWARE GROUPS AS CYBER PROXIES, PIRATES, AND PRIVATEERS, James Martin and Chad Whelan, State Crime Journal, 2023, Vol. 12, No. 1, Published by: Pluto Journals, P.5

(ISSN: 2537 - 0758)

cyberspace or the specific threats faced by women and gender minorities online.

This lack of specificity raises critical concerns about the Convention’s ability to deliver inclusive and effective justice, especially in light of empirical data provided by UN reports, which indicate that women and girls represent 65 percent of global trafficking victims, with more than 90 percent of identified female victims trafficked for the purpose of sexual exploitation. The absence of clear, enforceable mechanisms within the Convention to address gender-based cybercrime constitutes a significant gap in the international legal framework, and undermines efforts to create a comprehensive and equitable approach to cybercrime prevention and accountability On December 24, 2024, the UN General Assembly adopted the Cybercrime Convention, the first international criminal justice treaty of the 21st century. While largely welcomed as progress in global cybercrime cooperation, some states, including the United States, expressed reserved optimism, highlighting its potential to combat evolving cyber threats like ransomware, fraud, and intrusions, contingent on robust domestic safeguards.

However, the Convention inadequately addresses the gendered dimensions of cybercrime, neglecting the disproportionate impact of online sexual exploitation, harassment, and trafficking on women and girls. This omission contrasts starkly with earlier UN resolutions acknowledging the "feminization of poverty" as a factor in trafficking vulnerability. Despite general references to protecting vulnerable groups, the Convention lacks explicit recognition of gender-based cyber violence and the specific threats faced by women and gender minorities online.

This lack of specificity raises concerns about the Convention's ability to deliver inclusive justice. UN data indicates that women and girls constitute 65% of global trafficking victims,

with over 90% of identified female victims trafficked for sexual exploitation. The absence of clear, enforceable mechanisms to address gender-based cybercrime represents a significant gap in the international legal framework, hindering comprehensive and equitable cybercrime prevention and accountability([9]).

In a practical demonstration of the risks cybercrimes pose to women and children, the subsequent lines will detail the particulars of the following case:

In the case of State v. Ryan K. Manasco, the Louisiana Court of Appeal addressed a significant cybercrime involving the possession of child pornography. In March 2021, law enforcement executed a search warrant at Manasco's residence in DeSoto Parish, Louisiana, uncovering over 2,000 images and videos depicting severe child exploitation and bestiality. Manasco was initially charged with multiple counts, including possession and distribution of child pornography and sexual abuse of animals. Through a plea agreement, he pled guilty to two counts of possession of pornography involving juveniles under the age of 13, with other charges dismissed. The trial court sentenced him to 40 years at hard labor without benefits, suspending ten years and imposing five years of probation. However, the appellate court found the sentence illegally lenient, as Louisiana law mandates no suspension of sentences for such offenses. Upon resentencing, the court imposed two concurrent 30-year sentences at hard labor without benefits, emphasizing the gravity of the offense and the substantial benefit Manasco received from the plea deal. This case underscores the challenges in prosecuting cybercrimes and the

[9] GENDERING THE NEW INTERNATIONAL CONVENTION ON CYBERCRIMES AND NEW NORMS ON ARTIFICIAL INTELLIGENCE AND EMERGING TECHNOLOGIES, 2025, P.16, Rangita de Silva de Alwis, 20 Wash. J.L. Tech. & Arts 1

(ISSN: 2537 - 0758)

importance of adhering to statutory sentencing requirements to ensure justice ([10]).

A quick analysis of the details of this case reveals the evidence of a cybercrime being committed as follows:

Digital Forensic Evidence

Investigators executed a search warrant and seized electronic devices from the defendant's residence. A forensic analysis of these devices revealed over 2,000 files, including images and videos, depicting child sexual exploitation and bestiality. These digital files were central to establishing the nature and severity of the offense.

IP Address Tracing

Law enforcement traced illegal online activity to an IP address registered at the defendant’s home, providing probable cause for the search and connecting him to the criminal content.

File Metadata and Timestamps

The forensic examination included metadata showing download and access times, verifying that the materials were actively stored and accessed by the defendant, which supported the charge of knowing possession.

Volume and Nature of Content

The high volume and extremely graphic nature of the files found added weight to the prosecution's claim of intentional and repeated possession, rather than accidental or unknowing download.

These forms of evidence are typical in cybercrime cases and demonstrate how digital footprints, when properly collected and analyzed, serve as strong proof of criminal activity.

[10] Court of Appeal of Louisiana, Third Circuit, March 26, 2025, Decided, State v. Ryan,24-434, No Shepard’s Signal™

4 Cybercrime as a Threat to Intellectual Property Protection

Cybercrime poses a significant threat to intellectual property by enabling the unauthorized access, theft, and distribution of protected content. It undermines the economic value of innovation and creative work, discouraging investment in research and development. Moreover, it erodes trust in digital platforms and compromises the integrity of academic and commercial institutions.

An Overview of the Legal, Economic, and Social Implications of Intellectual Property Rights in Cyberspace([11]):

Legal Implications of Intellectual Property Rights in Cyberspace

Intellectual property rights (IPRs) are chiefly safeguarded through copyright and patent law. Copyright laws protect original works of authorship—including literary works, musical compositions, and software—while patent laws secure rights over inventions such as computer hardware and software. In cyberspace, these laws grant creators legal means to guard against the unauthorized use of their creations.

Specifically, the Digital Millennium Copyright Act (DMCA)([12]) serves as a key legislative tool for the protection

[11] Intellectual Property Rights in Cyberspace, by: Sankalp Mirani & Unnati Kanyal, International Journal of Engineering, Management and Humanities (IJEMH), Volume 5, Issue 1, Feb, 2024, p.314
www.ijemh.com

[12] The Digital Millennium Copyright Act (DMCA) was signed into law by President Clinton on October 28, 1998. The legislation implements two 1996 World Intellectual Property Organization (WIPO) treaties: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. The DMCA also addresses a number of other significant copyright-related issues.
The Digital Millennium Copyright Act (DMCA) is binding solely within the United States and applies to companies and individuals operating or conducting business there. However, due to the inherently global nature of the Internet, the

(ISSN: 2537 - 0758)

of digital content. It prohibits unauthorized reproduction, distribution, and sale of copyrighted material and introduces a "notice and takedown" procedure, allowing copyright owners to demand the removal of infringing content from websites. Additionally, the DMCA obliges online service providers to establish and enforce policies that terminate accounts of repeat copyright violators.

Overall, ensuring legal protection of intellectual property in cyberspace is vital for fostering the growth of digital innovation. It equips creators with the legal tools needed to safeguard their investments, encourages financial returns from their work, and promotes ongoing innovation and creativity.

Economic Implications of Intellectual Property Rights in Cyberspace

The enforcement of intellectual property rights in cyberspace carries considerable economic significance. By ensuring legal protections, creators are able to secure financial returns on their investments—whether through direct sales, licensing agreements, or royalty arrangements.

Furthermore, strong intellectual property protections incentivize companies to invest confidently in research and development without the risk of immediate imitation or theft of their products. This is particularly critical in the digital technology sector, where rapid innovation is essential.

Additionally, robust intellectual property systems foster competition by motivating companies to innovate and differentiate their offerings. This dynamic competition

influence of the DMCA has extended beyond U.S. borders. Many international companies, such as YouTube, Facebook, and Amazon, adhere to DMCA policies because their servers or headquarters are located within the United States. Additionally, several countries have indirectly aligned their domestic legislation with DMCA principles by amending their laws to comply with international agreements, such as the WIPO Copyright Treaty, which inspired several provisions found within the DMCA.

benefits consumers by expanding product choices and driving down prices, as businesses must continually strive to offer better goods and services to maintain their market positions.

Social Implications of Intellectual Property Rights in Cyberspace

The social consequences of intellectual property protection in cyberspace are equally significant. By enabling creators to reap financial rewards from their work, intellectual property rights not only support individual livelihoods but also promote cultural and technological advancement.

Moreover, they contribute to building an environment where creativity and innovation are valued and sustained, encouraging a more dynamic and diversified digital society.

A significant practical implication of the threat cybercrime poses to intellectual property rights lies in the case involving Aaron Swartz, the facts center on his unauthorized and systematic downloading of approximately 4.8 million academic articles from JSTOR through the Massachusetts Institute of Technology's (MIT) computer network. Although Swartz was a fellow at Harvard University and had lawful access to JSTOR via Harvard's library, he instead exploited MIT's more open network access policies for guests. Using a laptop registered under a fictitious name, "Gary Host," and later "Grace Host," Swartz bypassed JSTOR's and MIT's security measures, such as IP address blocks and MAC address restrictions, by repeatedly altering his digital identity and manipulating network configurations. Over the course of several months from September 2010 to January 2011, Swartz installed and used an automated script- -keepgrabbing.py-- to massively download JSTOR's content in violation of the organization's terms of use, thereby impairing JSTOR's servers and compromising access for legitimate users.

(ISSN: 2537 - 0758)

Despite JSTOR and MIT's escalating efforts to block his activity—including IP and MAC address blacklisting and physically securing network closets—Swartz continued his actions covertly, even going so far as to physically conceal his equipment in restricted spaces and obscure his identity on surveillance cameras. His actions ultimately led to JSTOR disabling MIT's access for multiple days, causing widespread disruption in academic access. The case drew significant attention not only for the technical and legal implications but also due to Swartz's intention to freely distribute the copyrighted material via public file-sharing platforms, framing the case within the broader debate about information freedom versus intellectual property rights ([13]).

This case highlights the tension between the ideals of open access to knowledge and the legal protections afforded to intellectual property in the digital age. Swartz's actions, while driven by a belief in the democratization of information, involved calculated, repeated breaches of legal and institutional security frameworks, resulting in substantial technical and reputational harm to JSTOR and MIT. It raises critical questions about the balance between ethical motivations and lawful conduct, emphasizing the need for clearer policies, legal frameworks, and open-access alternatives to minimize such conflicts in the future.

The Middle East, particularly Saudi Arabia and the United Arab Emirates, is experiencing significant financial losses due to cybercrime, with the average cost of a data breach reaching over $8 million per incident in 2023. This marks a sharp increase from 2018, when the average cost was $5.31 million. The rise is closely linked to the rapid digital transformation in the region, including the growth of e-commerce and

[13] JSTOR Evidence in United States vs. Aaron Swartz, https://docs.jstor.org/summary.html

widespread internet use, which has created more opportunities for cybercriminals. Despite high rankings in global cybersecurity indices, such as those published by the International Telecommunications Union (ITU), experts caution that these assessments rely heavily on self-reported data from the countries themselves. As a result, there may be a gap between the cybersecurity policies in place and their actual implementation. The increasing sophistication of cyber threats, combined with the Gulf states' expanding digital infrastructure, has made them particularly attractive and vulnerable targets. This suggests that while digital progress continues, the region's cybersecurity efforts may not be keeping pace with the risks ([14]).

5 Barriers to Cybersecurity Legislation

The internet has enabled the most radical democratization of speech yet, making it possible for anyone with an internet connection and a phone or computer to express themselves, connect with people regardless of geographical barriers, organize around shared interests, and share their experiences across the world in an instant

At every stage, speech has been further democratized, empowering people who could not previously make themselves heard and challenging the influence of the traditional gatekeepers of public information–including the state, the church, politicians, and the media. These advances have often been met first with excitement and enthusiasm, followed by a public backlash fueled by a mix of legitimate concerns about the impact of technology on society and moral panic stoked by the vested interests whose power has been

([14]) Why is the Middle East losing so much money to cybercrime? by: Andreas Illmer, Newstex Blogs, Deutsche Welle World September 3, 2024 Tuesday 8:25 PM EST,

(ISSN: 2537 - 0758)

challenged. In time, these pendulum swings have come to a resting point through a combination of the normalization of the technologies in society, the development of commonly understood norms and standards, and the imposition of guardrails through regulation ([15]).

Cybersecurity is about the security and digital sovereignty of every State, every company and every citizen. It is of major political, economic and social importance and must therefore be addressed from different angles: educational, legal and regulatory, social, technical, military, organizational, individual and collective, national and international.

Cybersecurity crimes are characterized by their difficulty in detection and proof since they involve hidden attacks that operate outside the tangible physical realm([16]).

In this paper, we will explain three important points that represent obstacles in the way of comprehensive legislative regulation to protect cybersecurity for all countries and the extent of their impact on the laws and legislation of the United Arab Emirates.

1. Rapid technological advancements outpacing legislative processes.

2. Conflicts between national sovereignty and cross-border jurisdiction.

3. Balancing individual privacy rights with national security concerns.

[15] The Future of Speech Online: International Cooperation for a Free and Open Internet, Nick Clegg, Daedalus , Summer 2024, Vol. 153, No. 3, The Future of Free Speech (Summer 2024),pp. 65-76, he MIT Press on behalf of American Academy of Arts & Sciences, Stable URL: https://www.jstor.org/stable/10.2307/48784941

[16] The Problem of Jurisdictional Conflict and the Applicable Law on Cybercrime, Hassan Yousef Magableh and Barjes Khalil Ahmad Al-Shawabkeh, Pakistan Journal of Criminology, September 2024 , Vol. 16; No. 3,

First: Rapid technological advancements outpacing legislative processes.

The rapid pace of technological innovation has revolutionized the digital landscape, introducing advanced tools and systems that enhance global connectivity and efficiency. However, this progress has also given rise to unprecedented cybersecurity threats, including data breaches, ransomware attacks, and the misuse of artificial intelligence. Unfortunately, legal frameworks often struggle to keep pace with these advancements. Traditional legislative processes are inherently slow, requiring extensive deliberation and approval, while technology evolves at an exponential rate. This lag creates significant gaps in regulation, leaving individuals, businesses, and governments vulnerable to cybercrimes. Moreover, the global nature of cyberspace poses additional challenges, as differing legal standards and enforcement mechanisms across jurisdictions hinder comprehensive solutions. To address this issue, a dynamic and adaptive legal approach is essential, combining real-time monitoring, international cooperation, and periodic updates to laws to effectively tackle emerging threats in cybersecurity.

Despite the development of the legislative organization to combat cybercrimes and protect cybersecurity in the Emirates through laws and ministerial decisions and the development of funding plans to secure cybersecurity, as a result of technological development, the Emirates has recently been experiencing a significant increase in cyberattacks, with an average of 50,000 daily incidents targeting various sectors, including government institutions, businesses, and critical infrastructure

Ransomware attacks: Between January and November 2024, the UAE reported 34 ransomware incidents, up from 27 in the entire year of 2023

(ISSN: 2537 - 0758)

In 2024, a cybercrime group attacked Etisalat, a major telecommunications provider in the UAE, using the LockBit ransomware, which led to the disclosure of confidential files([17]).

Second: Conflicts between national sovereignty and cross-border jurisdiction.

Cybercrime has an important and special dimension that distinguishes it from other crimes, which is that it is a crime that, in most cases, crosses national borders. This is due to the interconnected nature of global networks that allow a criminal in one country to commit a cybercrime with great ease and speed from his location, which may affect more than one victim in more than one country. In light of the current technological development, the effects of any action may be felt immediately in another place without any relation to geographical location at all. A transnational cybercrime may be committed by an entity that is not affiliated with a state or a governmental institution, and individuals, companies, governmental entities, non-governmental organizations, or other entities may be affected by the consequences of this crime([18]).

Cybercrime's global reach complicates its definition. Unlike most crimes, it often starts in one country and ends in another. Cloud computing has amplified cyber offenders' ability to transcend national borders. Differing cultural norms contribute to varying offense and enforcement patterns, likely influenced by differing definitions of cybercrime across countries. Cultural differences shape the definition of crimes like drug

[17] Middle East Insurance Review, 04 Dec 2024, positive Technology, https://global.ptsecurity.com/

[18] For more information on the conflict of jurisdiction of transnational crime and its impact on cybercrime, “Overcoming the conflict of jurisdiction in cybercrime”, Abdel monem Mohamed Magdy Khalifa, American University in Cairo, AUC Knowledge Fountain AUC Knowledge Fountain, 2020

offenses, prostitution, and domestic violence within specific jurisdictions, allowing criminologists to focus their definitions within those cultural boundaries. Cybercrime lacks this clear cultural boundary.

These differing definitions create challenges for international responses, impacting whether law enforcement becomes involved. Even beyond definitional issues, international police cooperation in addressing cybercrime is complex. Improved international cooperation promoting consistent definitions could enhance the response([19]).

The idea of digital sovereignty—which has gained so much attention lately—needs to be seen in the context of asserting state authority over the internet. However, in its manifold variations, the digital sovereignty discourse goes far beyond confirming and enforcing interventions by nation states in the digital space. The first and most prominent actor to call for more national sovereignty in digital matters was the Chinese government, which had been promoting both the preservation of territorial borders and the recognition of national governments as the dominant regulatory bodies since the early days of the global internet. In a 2010 white paper, it structured these various claims in the form of a strategy that seeks to protect Chinese "internet sovereignty", Today, digital sovereignty claims are no longer limited to (semi)authoritarian regimes.

Over the last decade, various liberal democracies made it their ambition to re-establish the nation state—including its citizens and the national economy—as a relevant category in the regulation and governance of the internet and of digital services. Most prominently, the EU has been developing and promoting a rather pronounced digital sovereignty discourse,

[19] The Palgrave Handbook of International Cybercrime and Cyber deviance, Defining Cybercrime, P.13, BrianK.Payne, June 2020

(ISSN: 2537 - 0758)

which continues to grow both in scope and in public acceptance. Within the European member states, the idea of digital sovereignty initially emerged in France and later in Germany where, since 2013, it has been structuring debates on digital matters not only among policy-makers but also quite prominently among nonstate actors from the private sector, academia, and civil society([20]).One of the most prominent governments seeking to impose control over cyberspace and control e-commerce is the Chinese government, which... launched a number of artificial intelligence (AI) and data protection regulations along with an antitrust crackdown on numerous platform companies. This aimed at bringing technological giants (namely platforms), capable of handling massive amounts of data and influencing people's everyday lives, under stricter government rule. While the Chinese government has only partially framed these actions within conceptual frameworks akin to 'digital sovereignty', the purported aim was accruing individual autonomy vis-à-vis big techs, arguably falling close to the EU's individual-level 'digital sovereignty' framework on a discursive level ([21]).

Third: Balancing individual privacy rights with national security concerns.

Cybersecurity has emerged as a global challenge and is becoming a tier one security threat for sovereign states. Heated debate rages in international forums concerning the rules of cyberspace, and the systemic and revolutionary

[20] From multi stake holderism to digital sovereignty: Toward a new discursive order in internet governance?, julia Pohle, Mauro Santaniello, Received: 17 April 2024 | Accepted: 18 August 2024
DOI: 10.1002/poi3.426, Policy Internet. 2024;1–20. wileyonlinelibrary.com/journal/poi3

[21] The false promise of individual digital sovereignty in Europe: Comparing artificial intelligence and data regulations in China and the European Union Riccardo Nanni , Pietro G. Bizzaro, Maurizio Napolitano, 8 September 2024, Policy Internet. 2024;1–16. wileyonlinelibrary.com/journal/poi3

challenges to global governance in cyberspace. particularly with respect to three issues.

First, the contradiction between cyber sovereignty and the spirit of the internet; the exclusivity of classical state sovereignty runs contrary to the spirit of the internet, which rests on the concept of unrestricted interconnectivity. If the emphasis is placed on cyber sovereignty, this may cause each country to set up a separate cyberspace of its own, thus resulting in the fragmentation of the internet.

Second, the contradiction between cyber sovereignty and human rights. This reflects the tension between the internet principle of freedom of speech, and state intervention in the name of cyber sovereignty, which restricts the free flow of information ([22]).

The third is the contradiction between cyber sovereignty and involvement of multiple stakeholders in governance. It is argued that cyber sovereignty will provoke controversy on the

([22]) In 2007, the National Security Agency (NSA) invaded Mr. Jamshid Makhtorov's privacy by monitoring him without a warrant, intercepting his emails and more than 3,000 audio recordings, and in 2012 he was charged with providing material support to terrorist organizations. The government alleged that Makhtorov communicated with members of the organization, expressing his support and willingness to join them in their fight.

Mr. Makhtorov's defense challenged the constitutionality of the surveillance methods used to gather evidence against him, arguing that they violated his Fourth Amendment rights, which guarantee the right to due process and protection from unreasonable searches and seizures.

Mr. Makhtorov is the first person to receive notice from the government that Section 702 had been used to spy on his communications and violate his privacy. In a split decision in December 2021, the 10th Circuit Court of Appeals ruled against Mr. Makhtorov, holding that protecting the nation from foreign threats outweighed concerns about due process violations.

United States v. Mahtorov, 20 F.4th 558, 581 (10th Cir. 2021).

(Human Rights Implications of the Use of New and Emerging Technologies in the National Security Space, Annabelle Bonnefont Global Center on Cooperative Security (2024), Stable URL: https://www.jstor.org/stable/resrep58515)

(ISSN: 2537 - 0758)

pattern of internet governance; that is, sovereign government-led governance will challenge the existing pattern of multi-party governance ([23]).

And with the surge of the digital sovereignty debate, countries and blocks in the world sought to build technological and regulatory capacity to ascertain technological autonomy—definitions notwithstanding. At the same time, these actors sought to position themselves discursively, differentiating their own understanding of digital sovereignty from that of competing powers). In this context, the European Union (EU) elaborated the concept of digital sovereignty as something obtainable on the individual level, where regulations are put in place purportedly for the users of digital technologies to be fully informed about an application's technical functioning and be able to choose what personal data (not) to share.

6 Emerging technologies and new risks

Emerging technologies refers to: “New and rabidly developing technologies with the potential to significantly impact society and industry. Characterized by:

Transformative potential, Ability to solve global challenges, Capacity to redefine the world ([24]).

Emerging technologies term is applicated on([25]):

(1) ARTIFICIAL INTELLIGENCE (AI);

(2) BIO-TECHNOLOGY;

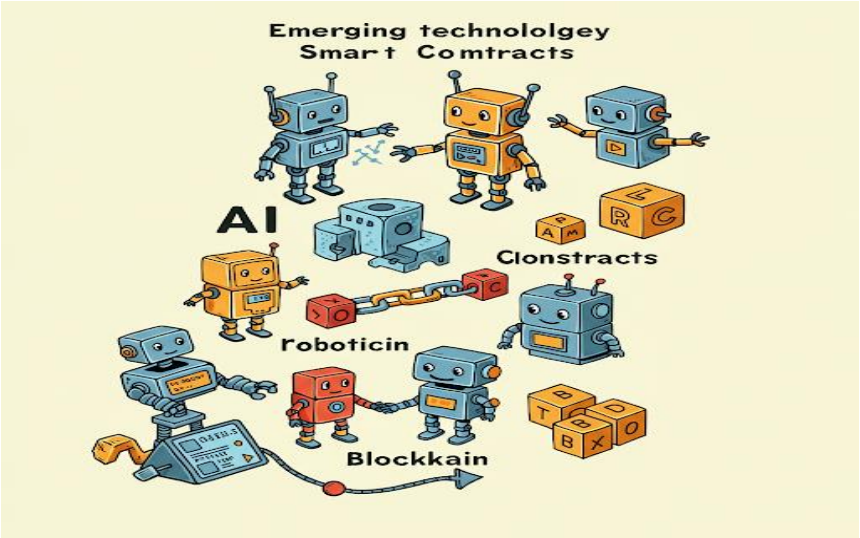
[23] A Three-Perspective Theory of Cyber Sovereignty, Hao Yeli , Vol. 7, No. 2, THE FIFTH DOMAIN (2017), pp. 108-115, Institute for National Strategic Security, National Defense University

Stable URL: https://www.jstor.org/stable/10.2307/26470523

[24] What is an emerging technology?, Daniele Rotolo , Diana Hicks , Ben R. Martin, Research Policy 44 (2015) 1827–1843

[25] Emerging Technologies: New Challenges to Global Stability, ROBERT A. MANNING, Atlantic Council, Scowcroft center for strategy and security (May-2020)

(3) BLOCKCHAIN;
(4) ROBOTICS;
(5) INTERNET OF THINGS;
(6) VIRTUAL AND AUGMANTED REALITY;
Which are shaping the future, promising to revolutionize industries,
solve global challenges, and redefine the way we live and interact with the world "THE FOURTH INDSTURAL REVLOUTION".



7 The UAE has adopted a policy based on the following axes:

- Issuing laws that criminalize cyber-attacks and regulate dealings through cyberspace.
- Issuing ministerial decisions that regulate what has not been issued by decree law.
- Developing and announcing national policies to ensure cloud security.
- Issuing applications and platforms for reporting cybercrime.

(ISSN: 2537 - 0758)

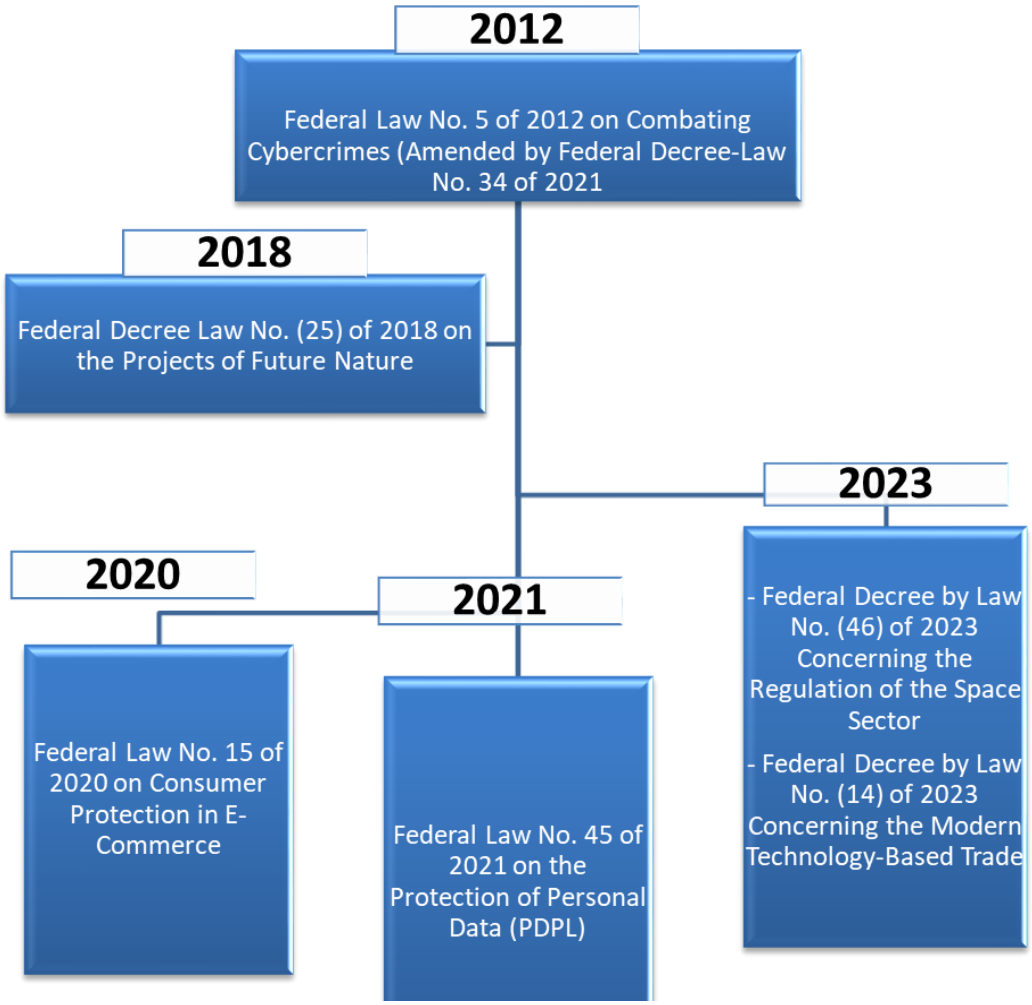
This paper will examine these axes in detail to illuminate the UAE's legislative efforts to enhance cybersecurity and assert its authority in safeguarding national security.

Legal Frameworks UAE:

First: laws that criminalize cyber-attacks and regulate dealings through cyberspace.

- **Federal Law No. 5 of 2012** on Combating Cybercrimes (Amended by Federal Decree-Law No. 34 of 2021): This is the primary law governing cybercrimes in the UAE, addressing unauthorized access, hacking, online fraud, and spreading fake news.
- **Federal Decree Law No. (25) of 2018** on the Projects of Future Nature.
- **Federal Law No. 15 of 2020** on Consumer Protection in E-Commerce: Addresses consumer rights for online transactions.
- **Federal Law No. 45 of 2021** on the Protection of Personal Data (PDPL): This law regulates personal data processing and ensures data privacy in compliance with global standards.
- **Federal Decree by Law No. (46) of 2023** Concerning the Regulation of the Space Sector, This Decree by Law aims to achieve the following: Organise Space Activities and other activities related to the Space Sector. Stimulate investment and encourage private and academic sector participation in the Space Sector and related activities. Support the implementation of the necessary safety, security and environmental measures to enhance the long-term stability and sustainability of Space Activities and related activities to the Space Sector. Support the transparency principle and the State commitment to implement the provisions of international conventions and treaties related to Outer Space and to which the State is a party.

UAE's cyber–Legislation Timeline



Second: ministerial decisions that regulate what has not been issued by decree law.

- **Cabinet Resolution No. (13) of 2023** Concerning the Committee for Preventing Cyber Threats and Malware.
- **Cabinet Resolution No. (111) of 2022** Regulating Virtual Assets and the Related Service Providers

(ISSN: 2537 - 0758)

Third: Developing and announcing national policies to ensure cloud security.

The UAE has developed a specific strategy to confront cyber threats **(**[26]**):**

The UAE's National Cybersecurity Strategy aims to create a secure and robust cyber infrastructure. It was updated, announced and implemented in 2019 by the Telecommunications Regulatory Authority (TDRA), the entity responsible for the ICT sector and digital transformation in the country.

The National Cloud Security Policy aims to ([27]**):**

Keep pace with global changes in the field of cybersecurity and the digital economy.

Secure and protect digital assets and cyberspace.

Enhance cloud security in line with the country's national priority.

Accelerate the pace of cloud services adoption in the region by facilitating government agencies and companies' access to data and information and exchanging them according to the best cybersecurity standards.

Establish a successful system that operates according to strict standards to build trust in the system of cybersecurity service providers in the country.

The following five cloud security principles have been developed to provide decision makers with the essential elements needed to drive the secure adoption of cloud services and their operations in the UAE. These principles help users, service providers, operations and procurement.

- A risk management-based approach.
- Data-driven cloud security where the degree of cloud security is aligned with the degree of data sensitivity, its impact on business and privacy expectations.

([1]) https://www.wam.ae/en/details/1395302769739

([2]) Public Policy Document, The National Cloud Security Policy, https://uaelegislation.gov.ae/en/policy/details/lsy-s-lotny-llamn-lsh-by

- A system based on collaboration and transparency.
- Continuously improve cloud security practices to ensure their suitability, efficiency and effectiveness.

- **The National Policy for the Internet of Things Security([28])**

in 2023, the Federal Government launched the National Policy for Internet of Things (IoT) Security to enhance the UAE's global standing in the field of IoT security and to support the protection of the UAE's cyberspace. This policy outlines the main directives for the cybersecurity system, assigning essential tasks and responsibilities to improve its operational capabilities, ensuring an optimal response to cyber incidents. this policy supports the adoption of emerging technologies, cloud computing, and the IoT. It also ensures that IoT service providers meet security requirements and guarantees a level of protection for all IoT users, when purchasing or using services. This aims to mitigate the potential negative impacts that can accompany reliance on modern technologies.

Fourth ([29]): Issuing electronic applications and platforms aimed at regulating electronic dealings between individuals and enabling reporting of any cybercrime.

- **- RZAM is** a browser designed to detect and block malicious websites. It scans website links and evaluates web pages for malicious content. RZAM can distinguish between malicious and legitimate websites without the need for human interaction or retrieving historical data from databases. RZAM supports the growth of the

[28] Public Policy Document, The National Policy for the Internet of Things Security, https://www.uaelegislation.gov.ae/en/policy/details/lsy-s-lotny-lamn-ntrnt-lashy

([2]) https://www.digitaldubai.ae/newsroom/news/dubai-electronic-security-center-upgrades-rzam-cybersecurity-app-to-strengthen-digital-security-standards-in-dubai

(ISSN: 2537 - 0758)

knowledge-based economy, encourages investment in the digital economy, and enhances digital resilience.

- **the 'eCrimes platform'** launched by the UAE's Ministry of interior, for reporting cybercrimes and electronic fraud in order to quickly confront and control it.
- **Aman service**- Abu Dhabi Police
- **The "'My Safe Society" app** launched by the UAE's federal Public prosecution, to protect the security of the United Arab Emirates by reporting electronic fraud crimes through it.

8 EGYPT Legal Framework

The Egyptian legislator formulated a number of laws that contribute to securing the Egyptian cyber domain as the case may be. In the following table, the set of Egyptian arsenal laws which controlling or related to the Egyptian cyber domain:

Law No.	Law Title	Regulates
82 of 2002	Intellectual property law	regulates intellectual property rights in Egypt, including patents, trademarks, copyrights, industrial designs..
10 of 2003	Telecommunication Regulation law.	Communications infrastructure and digitization work.
15 of 2004	E-signature law.	regulates electronic signatures and the establishment of the Information Technology Industry Development Agency (ITIDA) in Egypt, ensuring the legal validity of e-signatures and electronic transactions.
94 of 2015	Anti-terrorism law.	Combating terrorism through all methods (including the use of electronic means).
175 of 2018	Anti-cyber and information technology crimes law.	Combating crimes committed through electronic means.

163 of 2023	Establishment of the Central Intellectual Property Agency	It aims to develop the intellectual property system to ensure the achievement of sustainable development goals in Egypt. The Authority aims to regulate and protect intellectual property rights ("Intellectual Property") in Egypt, in line with Egypt's international obligations.

Egypt has recognized the importance of international cooperation in addressing cybersecurity challenges. As an active member of the International Telecommunication Union (ITU), Egypt proposed the establishment of the ITU Council Working Group on Child Online Protection, and chaired this working group from 2010 to 2017. Egypt has also participated in and hosted regional cyber trainings, cybersecurity conferences and workshops organized by international organizations such as the ITU and the Organization of Islamic Cooperation. The idea of developing an Egyptian framework for cybersecurity and critical information infrastructure protection began in 2007, within a working group at the Egyptian Ministry of Communications and Information Technology. The first step in implementation was the establishment of the Egyptian National Computer Emergency Readiness Team (EG-CERT) in April 2009. The EG-CERT is affiliated with the National Telecommunications Regulatory Authority (NTRA), and provides support to several entities in the ICT, financial, and government sectors, in order to help them address cybersecurity threats and deal with cyber incidents ([30]).

[30] Towards a National Cybersecurity Strategy: The Egyptian Case, Sherif HASHEM, CISM, Former Chairman of the Executive Bureau, Egyptian Supreme Cybersecurity Council, Cabinet of Ministers, SYSTEMICS,

(ISSN: 2537 - 0758)

Notes on the Egyptian legislative framework

Despite Egypt's efforts to align its legislation with the rise of cybercrimes, shortcomings remain in addressing these crimes and ensuring cloud security, as illustrated by:

- Weak enforcement of laws and regulations. While there are legal texts criminalizing cybercrimes, there is insufficient awareness of their effective application to mitigate these offenses.
- A lack of digital platforms for promptly reporting electronic fraud, coupled with a slow response to cybercrime, which requires different approaches compared to traditional crimes.
- Legislative development has not kept pace with technological advancements, particularly in the context of e-commerce and the global digital transformation.
- No executive regulations have been issued for the Personal Data Protection Law to date, despite the passage of more than five years since its issuance**.**

The launch of the National Cybersecurity Strategy 2023-2027([31]**)** is a very important step towards avoiding the flaws and criticisms directed at the Egyptian legislative system, as it depends on building an integrated legislative framework, strengthening national partnership, building strong and resilient cyber defenses, enhancing international cooperation, changing the culture of society regarding cybersecurity, encouraging scientific research, and enhancing innovation and growth.

The Egyptian government's approach continues in commendable attempts to support and establish strategies that support awareness among individuals and preserve their

[31] Prime Minister's Office, Ministry of Communications and Information Technology, National Cybersecurity Strategy

material and moral rights from electronic fraud by **launching the National Intellectual Property Strategy 2022-2027([32]).**
With a look at the controls that the strategy has clearly set, it aims to determine the mechanisms for governing the institutional structure of intellectual property through six sub-goals, namely:
Establishing a national intellectual property body that unifies the efforts of intellectual property departments and offices according to the latest methods of administrative structuring and institutional organization.
Supporting digital transformation and providing registration, deposit and registration services using modern technological means. Training and developing the human element in the intellectual property system. Linking the Egyptian Intellectual Property Authority with the rest of the state's entities and institutions. Enhancing the enforcement and respect of intellectual property rights. Maximizing Egypt's role in the global intellectual property system, and working to coordinate and cooperate with international entities and organizations.
Also appears the importance of Public-private partnerships in cybersecurity are collaborative arrangements between government authorities and private sector entities aimed at addressing cyber threats and enhancing national cyber resilience. These partnerships have become increasingly important as the cyber domain grows more complex, interconnected, and vulnerable. While not new, their relevance has surged due to the private sector’s control over most

[32] The Egyptian Intellectual Property Authority in Light of the New National Strategy. A Foresight Vision
Dr. Ahmed Saeed Ezzat Amer, Member of the Intellectual Property Protection Committee at the Supreme Council of Culture, Saturday, January 27, 2024, Legal Publications - Digital Archive.
https://manshurat.org/content/ljhz-lmsry-llmlky-lfkry-fy-dw-lstrtyjy-lwtny-ljdyd-rwy-stshrfy

(ISSN: 2537 - 0758)

critical infrastructure—such as energy, finance, and communications—and its technical expertise and innovation capacity. Meanwhile, the public sector provides legal authority, regulatory frameworks, international coordination, and access to intelligence and law enforcement tools. Together, these sectors can create effective synergies, improving threat detection, incident prevention, and system recovery, while also promoting shared standards, fostering innovation, and building public trust in cybersecurity efforts([33]).

9 Similarities in legislative approach:

The United Arab Emirates (UAE) and Egypt exhibit notable parallels in their legislative frameworks concerning cybercrime. Acknowledging the escalating risks associated with cyber offenses, both nations have enacted comprehensive legislation aimed at regulating online conduct, safeguarding national security, and preserving societal stability. The primary commonalities include:

1. **Prioritization of National Security and Societal Stability**

Both the UAE and Egypt prioritize cyber legislation as instruments for protecting national security, particularly against terrorism, espionage, and threats to public order. Their legal frameworks frequently criminalize online activities perceived as detrimental to the state or disseminating misinformation.

2. **Comprehensive Definitions and Extensive Scope**

The cybercrime laws of both countries employ comprehensive definitions, affording authorities considerable discretion in enforcement. This encompasses imprecise terminology such

[33] A BRIDGE TO ADVANCE GLOBAL CYBERSECURITY, 56 Tex. Tech L. Rev. 627, Spring, 2024, Ben Haklai

as "public morals," "national unity," and "public peace," which can be applied across diverse situations.

3. **Stringent Penalties and Criminalization**

Both nations impose severe penalties for a broad spectrum of cyber offenses, ranging from unauthorized system access and online financial crimes to content considered objectionable or prejudicial to state interests. Imprisonment and substantial financial penalties are frequently applied.

4. **Government Oversight of Digital Content**

Both countries empower the government with extensive authority to monitor and restrict websites, social media platforms, and digital content deemed harmful or illegal, including content critical of the government or religious principles.

5. **Integration with Existing Legal Statutes**

Cybercrime laws in both nations frequently intersect with established penal codes, particularly concerning defamation, blasphemy, and offenses against state institutions, effectively extending conventional legal doctrines to the digital sphere.

6. **Surveillance and Data Retention Mandates**

Service providers are often legally obligated to retain user data and furnish it to authorities upon request, thereby facilitating surveillance initiatives in both countries.

The legislative strategies of the UAE and Egypt demonstrate a shared objective: to assert governmental oversight over cyberspace, impose rigorous sanctions for infractions, and utilize cyber legislation to protect political, ethical, and social structures. While these laws address genuine threats such as cyber fraud and unauthorized system access, they also serve as mechanisms for upholding state authority within the digital environment.

(ISSN: 2537 - 0758)

10 Areas where one country outperforms the other

The UAE demonstrates a clear advantage over Egypt in combating cybercrime, particularly in the following areas:

- Technological readiness and law enforcement capacity:

The UAE possesses a more advanced technological infrastructure and better-resourced law enforcement agencies, enabling more efficient tracking, investigation, and prosecution of cybercrimes. Improved interagency coordination, particularly between the Telecommunications Regulatory Authority (TRA), the Digital Government, and the Cybersecurity Council, facilitates rapid response and proactive prevention measures.

The implementation of AI-powered surveillance tools and monitoring capabilities enhances the speed and accuracy of detecting and mitigating cyber threats.

- A comprehensive and modern legal framework:

The UAE's legal framework is modern and detailed, and is regularly updated to reflect evolving digital trends. Legislation includes emerging technological violations, such as deepfakes, cryptocurrency fraud, and the misuse of artificial intelligence. This flexibility ensures the legal framework's continuity and effectiveness in a rapidly evolving digital environment.

Egypt distinguishes itself from the UAE in the following aspects:

- Balancing the protection of personal freedom and human rights with judicial oversight:

Egypt's Anti-Cybercrime Law requires judicial orders to enforce certain measures, such as accessing personal data or blocking websites, ensuring certain legal controls. This ensures a better balance between state authority and legal rights, thus preserving individual rights.

- Focus on protecting critical infrastructure:

Egypt pays particular attention to protecting critical infrastructure, including banking, transportation, and energy systems, by defining specific preventive measures and obligations. This prioritizes preventing cyberattacks targeting essential services, a critical component of achieving national resilience.

- Public sector awareness initiatives:

Egypt has made significant efforts to raise public awareness through educational campaigns and initiatives about digital risks and security best practices. This aims to promote a culture of cybersecurity, which is essential for building sustainable, long-term cyber resilience.

11 Conclusion:

This research has demonstrated the increasing complexity and severity of cyber threats confronting both Egypt and the United Arab Emirates in the context of rapid technological advancement. Despite the legislative efforts undertaken by both states to address cybercrime, notable legal and practical gaps remain, particularly in responding to the dynamic and evolving nature of digital threats. The analysis reveals that while current frameworks provide a necessary foundation, they must be continuously updated and refined to effectively combat sophisticated cybercrimes, such as hacking, electronic fraud, and data breaches. Ensuring robust legal protection is imperative for securing personal rights, fostering trust in digital transactions, and supporting broader economic and societal stability.

Based on these findings, several recommendations are proposed. There is a pressing need to balance the issuance of new cybersecurity legislation with the continuous evolution of cybercrime techniques. Additionally, developing

(ISSN: 2537 - 0758)

comprehensive national policies aimed at enhancing public awareness, particularly in protecting personal data and shielding children from harmful online content, is vital. Establishing digital platforms and applications dedicated to public education and collaboration on cybersecurity risks can further strengthen national resilience. Moreover, fostering coordinated efforts between governmental bodies and private sector entities is essential for formulating an integrated cybersecurity strategy, particularly in view of the growing reliance on e-commerce and digital services

12 Recommendations

1- Balancing between issuing legislation regulating Egyptian cybersecurity and the development of technological crimes and electronic fraud methods.
2- Developing national policies to raise awareness among individuals to protect their personal data and protect children from exposure to harmful content on the Internet.
3- Creating electronic applications and digital platforms to raise awareness and cooperate on reducing the risks of cybercrimes.
4- Cooperation between government sectors and private sector companies to develop a strategy to support cybersecurity, especially in light of the development of e-commerce and services.

References

- Die strafrechtliche Verantwortlichkeit von Anbietern (innerhalb) sozialer Netzwerke by Maximilian Nussbaum, Duncker & Humblot GmbH, 2025.
- Internet Governance: Past, Present and Future by Wade Hoxtell and David Nonhoff, Global Public Policy Institute (GPPI), Konrad Adenauer Stiftung.
- Cybersecurity Private-Public Partnerships: A Bridge to Advance Global Cybersecurity by Ben Haklai, 56 Tex. Tech L. Rev. 627, Spring 2024.
- Cyber Security, Cyber Crime and Measures to Prevent in Libraries by Mr. Gulshan Kumar Sachdeva and Mr. Muksesh Sachdeva, CPJ Law Journal, Volume XVII, January 2025.
- The Palgrave Handbook of International Cybercrime and Cyber Deviance, Defining Cybercrime, p.9 by Brian K. Payne, June 2020.
- Hacking Through History by Jade Fell, Engineering & Technology, Volume 12, Issue 3, April 2017.
- Ransomware Through the Lens of State Crime: Conceptualizing Ransomware Groups as Cyber Proxies, Pirates, and Privateers by James Martin and Chad Whelan, State Crime Journal, 2023, Vol. 12, No. 1, Pluto Journals.
- Gendering the New International Convention on Cybercrimes and New Norms on Artificial Intelligence and Emerging Technologies by Rangita de Silva de Alwis, 20 Wash. J.L. Tech. & Arts 1, 2025.
- Intellectual Property Rights in Cyberspace by Sankalp Mirani and Unnati Kanyal, International Journal of Engineering, Management and Humanities (IJEMH), Volume 5, Issue 1, February 2024.
- JSTOR Evidence in United States vs. Aaron Swartz, https://docs.jstor.org/summary.html.
- Why is the Middle East Losing So Much Money to Cybercrime? by Andreas Illmer, Newstex Blogs, Deutsche Welle World, September 3, 2024
- The Future of Speech Online: International Cooperation for a Free and Open Internet by Nick Clegg, Daedalus, Summer 2024, Vol. 153, No. 3, The MIT Press on behalf of American Academy of Arts & Sciences.

(ISSN: 2537 - 0758)

- The Problem of Jurisdictional Conflict and the Applicable Law on Cybercrime by Hassan Yousef Magableh and Barjes Khalil Ahmad Al-Shawabkeh, Pakistan Journal of Criminology, September 2024, Vol. 16, No. 3.

- Overcoming the Conflict of Jurisdiction in Cybercrime by Abdel Monem Mohamed Magdy Khalifa, American University in Cairo, AUC Knowledge Fountain, Middle East Insurance Review, December 4, 2024, Positive Technology, https://global.ptsecurity.com/.

2020.

- The Palgrave Handbook of International Cybercrime and Cyber Deviance, Defining Cybercrime, p.13 by Brian K. Payne, June 2020.

- From Multi-Stakeholderism to Digital Sovereignty: Toward a New Discursive Order in Internet Governance? by Julia Pohle and Mauro Santaniello, August 2024, Policy Internet.

- The False Promise of Individual Digital Sovereignty in Europe: Comparing Artificial Intelligence and Data Regulations in China and the European Union by Riccardo Nanni, Pietro G. Bizzaro, and Maurizio Napolitano, September 8, 2024, Policy Internet.

- A Three-Perspective Theory of Cyber Sovereignty by Hao Yeli, Vol. 7, No. 2, The Fifth Domain (2017), Institute for National Strategic Security, National Defense University.

- What is an Emerging Technology? by Daniele Rotolo, Diana Hicks, and Ben R. Martin, Research Policy 44 (2015).

- Emerging Technologies: New Challenges to Global Stability by Robert A. Manning, Atlantic Council, Scowcroft Center for Strategy and Security, May 2020.

- Public Policy Document, The National Cloud Security Policy.

Towards a National Cybersecurity Strategy: The Egyptian Case by Sherif Hashem, CISM, Systemics, Cybernetics and Informatics, Volume 17, Number 3, 2019.

- The Egyptian Intellectual Property Authority in Light of the New National Strategy: A Foresight Vision by Dr. Ahmed Saeed Ezzat Amer, Legal Publications – Digital Archive, January 27, 2024.