Comprehensive approach to cybercrime prevention in Arab countries

Submitted: 1st May 2024
Reviewed: 31 May 2024
Revised: 20 July 2024
Accepted: 21 July 2024

Tsyplakova Alyona Dmitrievna*
https://orcid.org/0000-0001-8564-0696

Article submitted to peer blind review

Licensed under a Creative Commons Attribution 4.0 International

DOI: https://doi.org/10.26512/lstr.v17i1.53743

Abstract

[Purpose] Given the cross-border nature and technological specificity of cybercrime, international cooperation in combating it is of particular importance, based primarily on national regulation and a regional approach.

[Methodology/approach/design] This study is a descriptive investigation of cybercrime prevention in the Kingdom of Saudi Arabia, the United Arab Emirates, the Kingdom of Bahrain, the Sultanate of Oman, the State of Qatar, and the State of Kuwait (GCC member states) mainly based on genetic, systematic-functional and systematization methods. Strategies and policies as elements of criminal policy are reflected in Figures. Technical guidelines and standards as parts of cybercrime prevention are reflected in Tables.

[Findings] Chronologically (in the 2010s), computer emergency response teams (CERTs) were the first to be established, which later became accountable to competent authorities (cybersecurity centers) and developed guidance documents in various areas: strategies and policies, technical guidelines, and standards. An exception is the Sultanate of Oman, where a national strategy was approved by the highest official as early as 2003. Moreover, the coordinating bodies have come a long way and have evolved in terms of both competence and status. The focus of individual states on the development of subjects is evident. At the regional level, CERT and related committees have been established to update existing regulation and create platforms to counter electronic abuse. There are other core initiatives such as electronic ambassadors that contribute to cybercrime prevention.

Keywords: Cybercrimes. GCC. Arab countries. Crime prevention.

*Lecturer of the Department of Criminal Law, Criminal Procedure and Criminology Moscow State Institute of Foreign Relations (University) Ministry of Foreign Affairs of the Russian Federation. Address: 76, Prospect Vernadskogo Moscow, Russia, 119454. E-mail: tsyplakova.a.d@my.mgimo.ru.

INTRODUCTION

Cybercrimes can be described as both crimes of international nature and transnational ones. Taking into account the specifics of their technical issues and the subject-matter, international cooperation in combatting such offences is of high interest. In order to maintain it, one should understand national legislative specifics. Due to juridical techniques and linguistics matters, Muslim countries are challenging to analyze for scholars. The Cooperation Council for the Arab States of the Gulf, also known as the Gulf Cooperation Council (GCC), counts for 6 member-states that have elaborated complex substantive and procedural laws (Tsyplakova A.D., 2024). With the regard to the specific combination of religious and secular principles in the Arab legislation and linguistic specifics, the research contributes to filling the gaps in understanding modern anti-cybercrime regulation and initiatives.

The GCC highlights the following pillars of the so-called guiding legal framework (Arabic “ركائز الإطار القانوني الاسترشادي”): electronic communications (Arabic “الإتصالات الإلكترونية”), electronic transactions and electronic signatures (Arabic. “المعاملات الإلكترونية والتوقيعات الإلكترونية”), data protection and privacy (Arabic “حماية البيانات والخصوصية”), electronic crime (Arabic. “الجرائم الإلكترونية”), intellectual property protection (Arabic “حماية الملكية الفكرية”), electronic content (Arabic “المحتوى الإلكترونية”), electronic payment system (Arabic. “ نظام الدفع الإلكتروني”), consumer or beneficiary protection (Arabic “ حماية المستهلك او المستفيد”), and Internet and IT governance (Arabic “ الإنترنت وحوكمة تكنولوجيا المعلومات”)[1]. Taking into account the diversity of legal regulators, it is proposed to streamline the “cyberlaw” the recommendation documents and bylaws, divided into the following areas: regulation of the telecommunications sector (licensing, provision of certified services, rules for the use of social networks, communication and publication, including electronic advertising and content); development of electronic document management and commerce, virtual assets, use of artificial intelligence; protection of personal data protected by the law; protection of personal data, and electronic advertising and content.

Chronologically (since 2007), the first means of ensuring cybersecurity in the Arab States was of a criminal law nature - criminalization of acts. Despite the content of the word “combat” (Arabic “مكافحة”) in the titles of the acts, they are not related to this form of influence on crime, as it is a criminal law means of cybersecurity, i.e., criminalization.

[1] Portal of the Cooperation Council for the Arab States of the Persian Gulf. Guiding legal framework. http://www.gcc-egov.org/web/guest/laws;jsessionid=B5AC15C1BAC7D86B98BCC5A668E5D826.

Unlike the rest of the Arab countries, which only in the mid-2010s tasked the established competent authorities to develop policies in this area, the Sultanate adopted a strategy as early as 2003, which anticipated even the 2007 Saudi Regulation. Moreover, it was approved by the Council of Ministers, headed by the Sultan, the head of state, who is in fact the highest official. This indicates a combined approach due to the combination of different forms of influence on cybercrime.

Chronologically, the next step in countering cybercrime was the establishment of CERTs and the adoption of national policies. More recently, central competent authorities have been established, but the bureaucracy is relatively small compared to the United States, although the United Arab Emirates and the State of Qatar have larger bureaucracies than other countries in the Arabian zone.

METHODOLOGY

The study is based on content analysis of documents, special-legal methods such as interpretation and formal-legal method, methods of juris linguistics and consider comparative in nature. Authentic sources in Arabic prevail. Using the systematization, the author has summarized core provisions of strategies, visions, guidance and standardization documents.

GUIDANCE DOCUMENTS AND INSTITUTIONAL MECHANISMS

Regional level

Scholars suggest that the Gulf Cooperation Council has a strategy to combat cybercrime (Salem F., Fiscbach T., 2017). However, only a comprehensive scientific study on “Electronic Crimes in the Gulf Society and How to Counter them” was conducted by the winner of the 2015 Prince Naif bin Abdulaziz Prize for Security Research in Sultan Qaboos Academy of Police Sciences (Sultanate of Oman, Nizwa) (General Secretariat of the Cooperation Council for the Arab States of the Persian Gulf, 2016).

There is neither a unified strategy within the GCC, nor a bureau (Arabic “مكتب”), union (Arabic “اتحاد”) or office (Arabic “جهاز”) (Nir R., Clark R., 2011). Such practice is actively implemented within the framework of the Organization of Islamic Cooperation (Aljarida, 2023). As early as 2011, the issue was raised in Arabic doctrine. On 10.02.2017, GCCPol (Arabic “جهاز الشرطة الأمن الخليجية”) held joint meeting with cybersecurity committee of the General Secretariat of the Council (Arabic “جنة الأمن السيبراني بدول مجلس التعاون”) previously established and conducted a cyber drill (Alkhaleej, GCC General Secretariat). On 23.10.2022 the e-government executive committee, the committee of postal and telecommunication agencies and the ministerial committee on cybersecurity held their first meetings (Oman News Agency).

National Level

Governing documents

Vision (Arabic “رؤية”) refers to the national strategy for the development of the state and individual sectors, which specifies the goals and initiatives under which individual projects and programs are implemented. In 2021, the UAE also developed the UAE Centennial 2071 plan (Arabic “مئوية الإمارات ٢٠٧١”)[2].

While the GCC Member States' Visions only focus on general digitalization issues, national cybersecurity strategies have been adopted by authority bodies such as ministries, commissions, or directorates. It is believed that Qatar was one of the first countries to adopt a cybersecurity strategy in 2013 and KSA was the latest in 2020. The UAE has also developed a separate document in addition to the federal level in the Emirate of Dubai (Shires J., Hassib B., 2022). At first glance, one has not found the described concept only in the Sultanate of Oman, although there are plenty of relevant initiatives, guidelines, and policies. This may be due to the fact that the responsible authority was initially tasked with drafting a law on combating information technology crimes. And the first step is often the criminalization, which in turn refers to criminal law means of ensuring cybersecurity.

Nevertheless, the Digital Oman Strategy was actually adopted back in 2003 and updated in 2010. Long-lasting modernization has taken place: the National Broadband Strategy in 2014, the Digital Oman 2030 (eOman) Strategy in 2017, the National Digital Economy Program, the State Digital Transformation Program and the National Artificial Intelligence and Advanced Technology Program in 2020, and the National Data Strategy in 2022[3].

[2] UAE. UAE CENTENNIAL PLAN 2071. https://uaecabinet.ae/en/uae-centennial-plan-2071.

[3] Ministry of Transportation, Communications and Information Technology of the Sultanate of Oman. National Digital Economy Program. https://ita.gov.om/ITAPortal_AR/Our_Projects/Our_Projects_List.aspx?svc=657&NID=170001&Odt=37. Ministry of Transportation, Communications and Information Technology of the Sultanate of Oman. National Artificial Intelligence and Advanced Technology Program. https://mtcit.gov.om/ITAPortal_AR/Our_Projects/Our_Projects_List.aspx?svc=657&NID=170035&Odt=37.

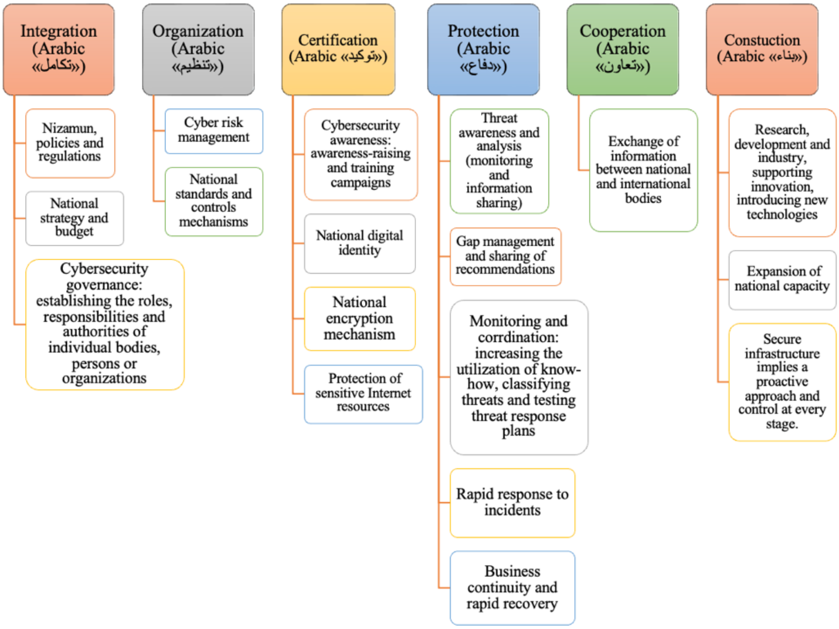
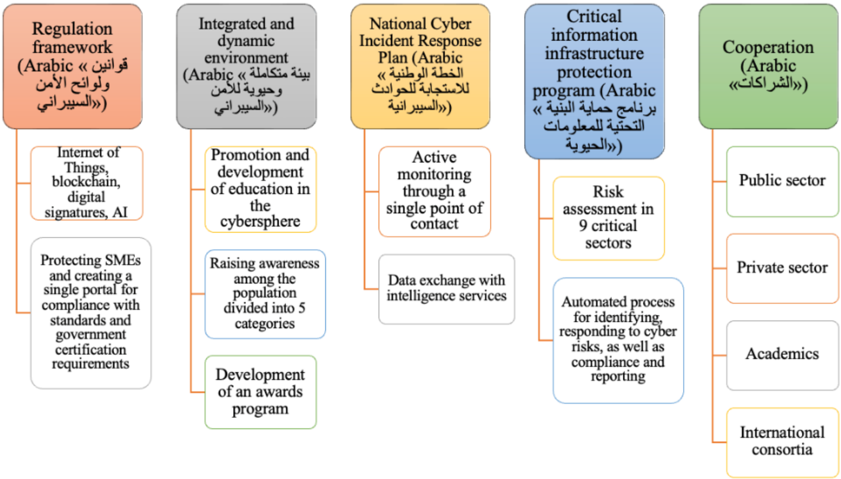

Integration (Arabic «تكامل»)
Nizamun, policies and regulations
National strategy and budget
Cybersecurity governance: establishing the roles, responsibilities and authorities of individual bodies, persons or organizations
Organization (Arabic «تنظيم»)
Cyber risk management
National standards and controls mechanisms
Certification (Arabic «توكيد»)
Cybersecurity awareness: awareness-raising and training campaigns
National digital identity
National encryption mechanism
Protection of sensitive Internet resources
Protection (Arabic «دفاع»)
Threat awareness and analysis (monitoring and information sharing)
Gap management and sharing of recommendations
Monitoring and corrdination: increasing the utilization of know-how, classifying threats and testing threat response plans
Rapid response to incidents
Business continuity and rapid recovery
Cooperation (Arabic «تعاون»)
Exchange of information between national and international bodies
Constuction (Arabic «بناء»)
Research, development and industry, supporting innovation, introducing new technologies
Expansion of national capacity
Secure infrastructure implies a proactive approach and control at every stage.

Figure 1 – Saudi cybersecurity strategy (2020)[4]


Regulation framework (Arabic « قوانين ولوائح الأمن السيبراني»)
Internet of Things, blockchain, digital signatures, AI
Protecting SMEs and creating a single portal for compliance with standards and government certification requirements
Integrated and dynamic environment (Arabic « بيئة متكاملة وحيوية للأمن السيبراني»)
Promotion and development of education in the cybersphere
Raising awareness among the population divided into 5 categories
Development of an awards program
National Cyber Incident Response Plan (Arabic « الخطة الوطنية للاستجابة للحوادث السيبرانية»)
Active monitoring through a single point of contact
Data exchange with intelligence services
Critical information infrastructure protection program (Arabic « برنامج حماية البنية التحتية للمعلومات الحيوية»)
Risk assessment in 9 critical sectors
Automated process for identifying, responding to cyber risks, as well as compliance and reporting
Cooperation (Arabic «الشراكات»)
Public sector
Private sector
Academics
International consortia

[4] KSA National Cybersecurity Authority. National Cybersecurity Strategy. https://nca.gov.sa/strategic.

Figure 2 – Emirati cybersecurity strategy (2019)

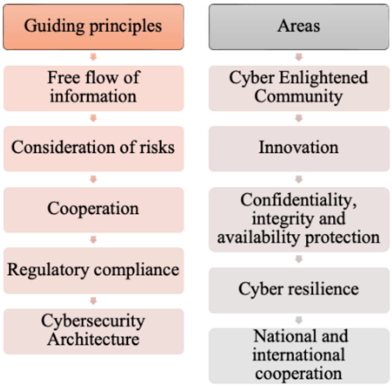

Guiding principles
Free flow of information
Consideration of risks
Cooperation
Regulatory compliance
Cybersecurity Architecture
Areas
Cyber Enlightened Community
Innovation
Confidentiality, integrity and availability protection
Cyber resilience
National and international cooperation

Figure 3 – Dubai cybersecurity strategy (2017)

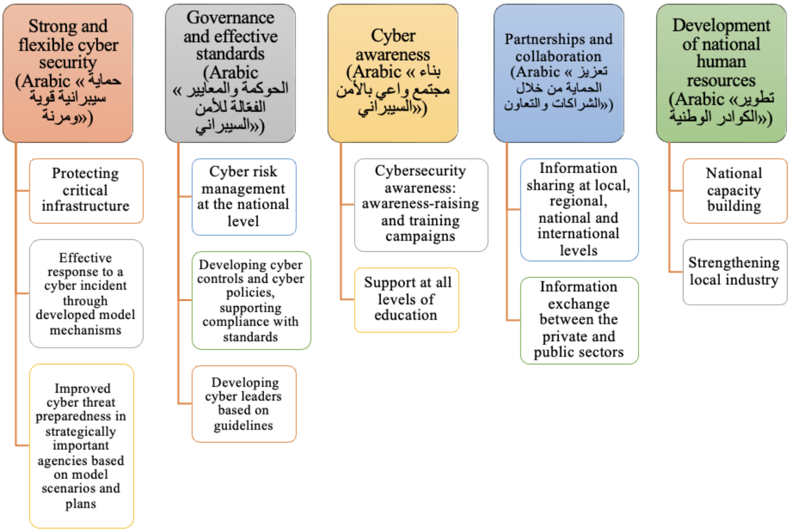

Strong and flexible cyber security (Arabic « حماية سيبرانية قوية ومرنة»)
Protecting critical infrastructure
Effective response to a cyber incident through developed model mechanisms
Improved cyber threat preparedness in strategically important agencies based on model scenarios and plans
Governance and effective standards (Arabic « الحوكمة والمعايير الفعّالة للأمن السيبراني»)
Cyber risk management at the national level
Developing cyber controls and cyber policies, supporting compliance with standards
Developing cyber leaders based on guidelines
Cyber awareness (Arabic « بناء مجتمع واعي بالأمن السيبراني»)
Cybersecurity awareness: awareness-raising and training campaigns
Support at all levels of education
Partnerships and collaboration (Arabic « تعزيز الحماية من خلال الشراكات والتعاون»)
Information sharing at local, regional, national and international levels
Information exchange between the private and public sectors
Development of national human resources (Arabic «تطوير الكوادر الوطنية»)
National capacity building
Strengthening local industry

Figure 4 – Bahraini cybersecurity strategy 2017[5]

[5] National Cybersecurity Center of the Kingdom of Bahrain. National Cybersecurity Strategy. https://www.ncsc.gov.bh/ar/national-strategy.html.

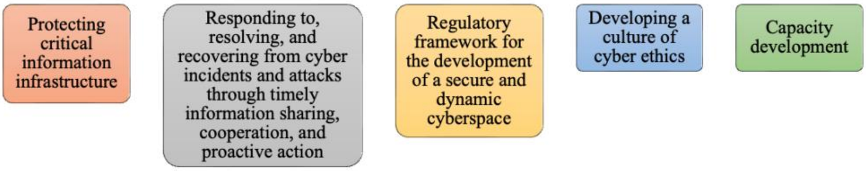

Protecting critical information infrastructure
Responding to, resolving, and recovering from cyber incidents and attacks through timely information sharing, cooperation, and proactive action
Regulatory framework for the development of a secure and dynamic cyberspace
Developing a culture of cyber ethics
Capacity development

Figure 5 – Qatari cybersecurity strategy 2014[6]

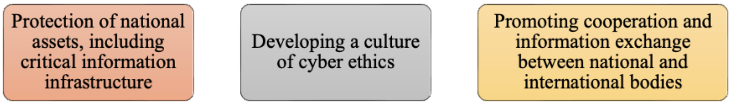

Protection of national assets, including critical information infrastructure
Developing a culture of cyber ethics
Promoting cooperation and information exchange between national and international bodies

Figure 6 – Kuwaiti cybersecurity strategy 2017–2020

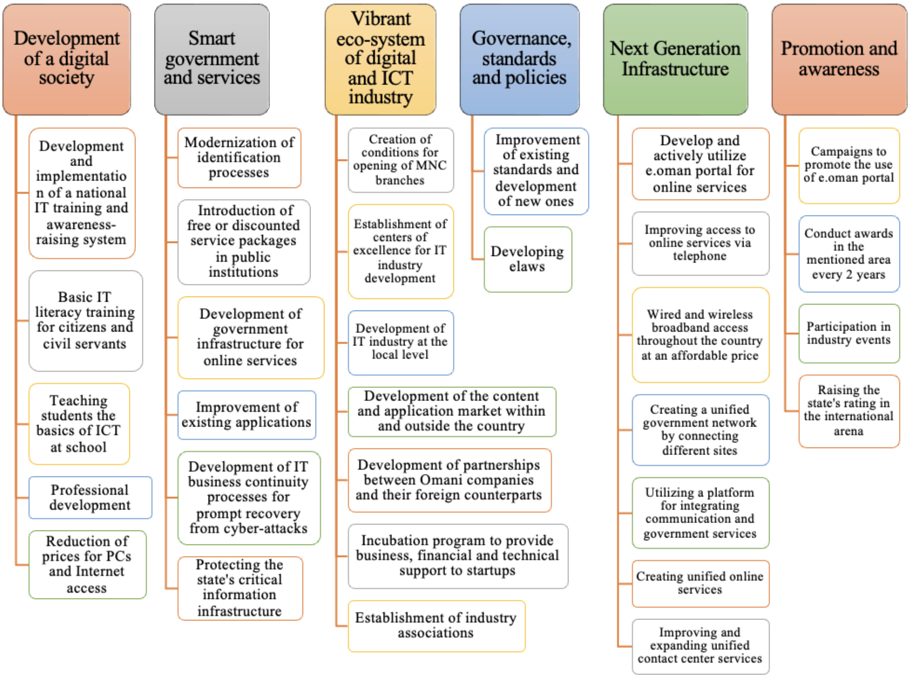

Development of a digital society
Development and implementatio n of a national IT training and awareness-raising system
Basic IT literacy training for citizens and civil servants
Teaching students the basics of ICT at school
Professional development
Reduction of prices for PCs and Internet access
Smart government and services
Modernization of identification processes
Introduction of free or discounted service packages in public institutions
Development of government infrastructure for online services
Improvement of existing applications
Development of IT business continuity processes for prompt recovery from cyber-attacks
Protecting the state's critical information infrastructure
Vibrant eco-system of digital and ICT industry
Creation of conditions for opening of MNC branches
Establishment of centers of excellence for IT industry development
Development of IT industry at the local level
Development of the content and application market within and outside the country
Development of partnerships between Omani companies and their foreign counterparts
Incubation program to provide business, financial and technical support to startups
Establishment of industry associations
Governance, standards and policies
Improvement of existing standards and development of new ones
Developing elaws
Next Generation Infrastructure
Develop and actively utilize e.oman portal for online services
Improving access to online services via telephone
Wired and wireless broadband access throughout the country at an affordable price
Creating a unified government network by connecting different sites
Utilizing a platform for integrating communication and government services
Creating unified online services
Improving and expanding unified contact center services
Promotion and awareness
Campaigns to promote the use of e.oman portal
Conduct awards in the mentioned area every 2 years
Participation in industry events
Raising the state's rating in the international arena

Figure 7 – Omani cybersecurity strategy 2003/2010

[6] George Washington University. Qatar National Cyber Security Strategy. May 2014. https://nsarchive.gwu.edu/sites/default/files/documents/3903662/Qatari-Government-Qatar-National-Cyber-Security.pdf.

Interestingly, although the Saudi legislator adopted the concept of cybersecurity later than other GCC countries, in 2012, Naif bin Ahmed bin Abdulaziz Al-Saud, prior to the cyberattack on state-owned Saudi Aramco, considered the need to adopt a relevant document based on the American experience (Al-Saud N. B. A, 2012).

In addition to the national cybersecurity strategy, other strategies are also being developed in related areas: artificial intelligence, e-government, the Internet of Things, blockchain and electronic document management[7]. The first two initiatives are being implemented by the competent ministry of Qatar in 2020. Relying on Islamic philosophy, aspirations to improve various sectors through AI (English “AI+X”, Arabic “اعتماد الذكاء الاصطناعي”) are noted. During the period 2017-2023, the UAE has updated several e-security provisions through the adoption of new policy documents: the UAE AI Strategy 2031 in 2017, the National Strategy for Advanced Innovation in 2018, the Digital Economy Strategy in 2022, the National e-Government Strategy 2025, the National Digital Quality of Life Policy, and the 2023 e-participation strategy.

Moreover, Dubai takes the lead in terms of areas covered: autonomous transportation strategy, 3D printing strategy, data strategy, cybersecurity strategy, blockchain strategy, Internet of Things strategy, electronic document management strategy (literally from Arabic “للمعاملات اللاورقية” paperless), e-commerce strategy, and smart Dubai strategy 2021. Abu Dhabi and Ajman have one initiative each: e-transformation and digital master plan 2017-2022 respectively[8].

[7] Ministry of Communications and Information Technology of the State of Qatar. Artificial Intelligence Strategy of the State of Qatar. https://mcit.gov.qa/sites/default/files/strtyjy_qtr_lwtny_fy_mjl_ldhk_lstny.pdf. Ministry of Communications and Information Technology of the State of Qatar. The e-government strategy of the State of Qatar 2020. https://mcit.gov.qa/sites/default/files/qatar-e-government-2020-strategy-ar_0.pdf.

[8] The UAE Telecommunications and Digital Regulatory Authority. National Cybersecurity Strategy. https://tdra.gov.ae/ar/national-cybersecurity-strategy. UAE. Cybersecurity and digital security. https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security. UAE. Digital Participation Strategy. https://u.ae/en/about-the-uae/digital-uae/digital-inclusion/national-digital-participation-strategy. UAE. Dubai Autonomous Transportation Strategy. https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/transport-and-infrastructure/dubai-autonomous-transportation-strategy. UAE. Dubai Data Strategy.

There are similar strategies, guidelines, policies, and models in the Sultanate of Oman and the list can be extended: information security framework, Cloud First policy, IT service continuity platform, national broadband strategy, basic security control guidelines, cloud governance framework, cybersecurity governance guidelines, data and information systems security classification map, ICT remote access policy, e-voting policy, government policy on open data, social media policy, IT risk management framework, reference models, design standards

https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/dubai-data-strategy. UAE. Smart Dubai 2021 Strategy. https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/strategies-plans-and-visions-untill-2021/smart-dubai-2021-strategy. UAE. Dubai eCommerce strategy. https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/dubai-e-commerce-strategy. UAE. Dubai Internet of Things Strategy. https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/strategies-plans-and-visions-untill-2021/dubai-internet-of-things-strategy. UAE. Dubai 3D Printing Strategy. https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/industry-science-and-technology/dubai-3d-printing-strategy. UAE. National Policy for Quality of Digital Life. https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/policies/government-services-and-digital-transformation/national-policy-for-quality-of-digital-life. UAE. National Strategy for Advanced Innovation. https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/innovation-and-future-shaping/national-strategy-for-advanced-innovation. UAE. The Dubai Cyber Security Strategy — Updated. https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/dubai-cyber-security-strategy. UAE. The UAE Digital Government Strategy 2025. https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/uae-national-digital-government-strategy. The UAE Ministry of Artificial Intelligence, Digital Economy and Remote Work. UAE National Strategy for Artificial Intelligence 2031. https://ai.gov.ae/wp-content/uploads/2021/07/UAE-National-Strategy-for-Artificial-Intelligence-2031-AR.pdf. Digital Dubai. Dubai Blockchain Strategy. https://www.digitaldubai.ae/initiatives/blockchain. Digital Dubai. Dubai Paperless Strategy. https://www.digitaldubai.ae/initiatives/paperless. Electronic Security Center in Dubai. Standards and policies. https://www.desc.gov.ae/ar/regulations-ar/standards-policies-ar/.

for websites and government e-service portals, guidelines for child protection on the Internet, database security standards and an IT governance charter, and project management documents[9].

In the case of KSA and Bahrain, one should address technical guidelines and standards, including those related to domain name registration, communication services, online banking, user interfaces, spam mitigation controls, social media usage, cell phone usage, cell phone software, and cryptocurrency.

National strategies also take into account critical infrastructure sectors. Bahrain, for example, identifies fuel and energy, financial services, information and telecommunications technology, health, public services, industry and transportation [10]; Qatar, in addition to banking, utilities, food, media and hazardous materials, with energy, finance and public services at the top of the list. Kuwait's National Strategy specifies the components of the fuel and energy complex (oil, water and electricity) and emphasizes the military-industrial complex (Sherin O., 2013).

Governing authorities

As for organizational issues, the Arab states have designated cybersecurity policy authorities, but they are not the only coordinating bodies. The largest bureaucracy is found in two countries:

- Qatar: the Computing Research Institute, the Expert Risk Commissions, the National Cybersecurity Committee, the Cybercrime Investigation Center, the National Cybersecurity Bureau - National Cyber Governance and Assurance, the Artificial Intelligence Regulatory Committee, the Communications Regulatory Authority, the Digital Incubation Center, and the Ministry of Communications and Information Technology (replaced the High Council for Communications and Information Technology);

- the UAE: the Telecommunications Regulatory Authority and Digital Government Authority (UAE Authority), Digital Wellbeing Council, e-Security Ambassadors, e-Security Center (Dubai), Signal Intelligence Authority (formerly the National Directorate for Electronic Security), Cyber Security Council, Artificial Intelligence and Blockchain Council and Digital Certification Center (Seeger R.).

The difficulty arises from English translation and authentic name of the bodies. For instance, the Cybercrime Investigation Center is now the Economic

[9] Omanuna. Policies, strategies and guidlines. https://oman.om/en/policies-strategies-and-guidlines.

[10] National Cyber Security Center of the Kingdom of Bahrain. Vital Sectors in the Kingdom of Bahrain. https://www.ncsc.gov.bh/ar/services/CNI-sectoral.html.

and Electronic Crimes Unit of the General Directorate of Criminal Investigations of the Ministry of Interior of the State of Qatar, similar to the Electronic Crime Department of the Police (Ministry of Interior) of the State of Kuwait.

It is important to note that while the General Authority for Communications and Information Technology of the State of Kuwait is similar in nature to the UAE Authority, its competence also covers certification activities, protection of the interests of users and service providers, which in the UAE is carried out by other and different bodies. There is a trend toward centralization of cybersecurity governance and regulatory bodies with clearly defined competencies, unlike in the United States (Shestak V., Tsyplakova A., 2023).

Other initiatives to combat cybercrime

For both the private sector and critical infrastructure institutions, the designated authorities and GCC-CERT develop standards, certification and licensing procedures, risk assessment body recognition and guidelines for the quality management system, security controls, data and information system security classification, free and open source software, user and database privacy regulation, rules and requirements for IT service providers.

Areas	**Themes**
Corporate information security	Corporate information security
	Corporate Information Security Responsibilities
Information security management	Malware protection
	Information Asset Management
	Information security monitoring
	Information security risk management
	Incident Management
	Policy Management
	Physical and environmental security
	Awareness
	Personnel
	Access Management
Management of information security issues	Information systems acquisition and development
	Change Management
	Backup and recovery
	Electronic Services
Compliance	Legal requirements

	Adopted policies and procedures
	Information security assessment
	Information security audit
External parties	Clientele
	Third party delivery management
	Outsourcing Service Provider
Others	Enterprise Operations Management
	Electronic media
	Document security
	Confidentiality
	Acceptable Use
	Fraud and whistleblowers

Table 1 – Standardization by the competent authorities of the GCC member states

Sometimes they are organized and collected on one service like Bh-CERT's “MITRE ATT & CK” matrix supplement.

The GCC Standards Organization lists the Arabic versions of ISO 27001 cybersecurity standards published in 2009 and 2015. Notably, the UAE has published its own information assurance standards (IAS) based on the 2005 and 2013 versions of ISO 27001 and the 2014 U.S. NIST Cybersecurity Framework.

Arab legal doctrine notes the problem of non-reporting of cyber incidents (Alzubaidi A., 2021). For this reason, cooperative efforts are actively building databases for information sharing. This is facilitated by Computer Emergency Response Teams (CERTs), which receive vulnerability complaints and cyber incident alert requests, develop recommendations, conduct information security seminars, conduct audits, and provide cyber security education; the GCC has also developed a mechanism (GCC-CERT) (Mishaal Abdullah bin Hussein). They are established as structural units of the National Cybersecurity Centers. The situation is similar in Bahrain; the KSA has changed the subordination of CERT (from the Telecommunications and Information Technology Commission to the National Cybersecurity Authority currently referred to as the Communications, Space and Technology Commission with a broader mandate). It has also developed a uniform form of measuring cybersecurity maturity to assess against three indicators: processes, practices, and people (Arabic “ البرنامج الوطني لقياس نضج الأمن السيبراني”) - which can be considered a model for others.

№	**Key pillars**	**№**	**Components**
1	Cybersecurity management	**1**	Cybersecurity strategy
		2	Cybersecurity management
		3	Cybersecurity policies and procedures
		4	Cybersecurity roles and responsibilities
		5	Cybersecurity risk management
		6	Compliance with cybersecurity legislation, regulations and standards
		7	Periodic cybersecurity audit and review
		8	Human resources cybersecurity
		9	Cybersecurity awareness and training programs
		10	Cybersecurity architecture
2	Ensuring cybersecurity	**1**	Asset Management
		2	Managing credentials and authorizations
		3	Network security management
		4	Mobile device protection
		5	Data and information protection
		6	Encryption and key management
		7	Backup data management
		8	Vulnerability management
		9	Network, computer, or cyber penetration testing
		10	Incident report management and cybersecurity monitoring
		11	Cybersecurity threat management
		12	Financial security
		13	Application security
		14	Customization and change management
		15	Remote working
		16	Medium security
3	Cybersecurity resilience	**1**	Cybersecurity resilience in business/body management
4	Third-party cybersecurity	**1**	Third-party cybersecurity

Table 2 – Structure of a Uniform Cybersecurity Maturity Measurement Form for the Saudi National Cybersecurity Authority

It is worth noting that although Arab countries adopted national strategies in the second half of the 2010s, CERTs were established much earlier (Q-CERT in 2005, SA-CERT in 2006, aeCERT in 2007, OCERT in 2010, Bh-CERT and Kw-CERT in 2012).

For the time being, at the regional level, the GCC e-Government Executive Committee has launched the Suspicious Internet Address System “IP Reputation” (Arabic “نظام عناوين الانترنت المشبوهة”), which allows computer emergency response centers to track suspicious Internet addresses around the world to prevent cyber threats[11].

In terms of organization, the UAE Telecommunication Regulatory Authority and Digital Government's initiative is e-Security Ambassadors who train students to promote aeCERT activities. A similar program is also being implemented in Oman, but its audience is broader: IT professionals (professional ambassadors), students (academic ambassadors) and citizens or residents of the Sultanate (information security ambassadors)[12]. Arab scholars highlight the problems with cybersecurity education (Alqurashi R. K., AlZain M. A., Soh B., Masud M., Al-Amri J., 2020). For this reason, a similar initiative should be implemented in Qatar, Saudi Arabia, and Bahrain.

In the Kingdom of Saudi Arabia (KSA) there are currently CyberHub (Arabic: “سايبرهب”)[13] with the support of the Saudi Federation for Cyber Security, Programming and Drones (SAFCSP)[14], CoderHub (كودرهب) (for programmers)[15] and Tuwake (طويق)[16] training camps on programming, cybersecurity, data science, for youth and 7/7. Under SAFCSP the first Middle East vulnerability detection rewards platform “Bug Bounty” (Arabic منصة مكافآت الثغرات) was established[17]. Such experiences are also of interest for implementation in other countries.

[11] Bahrain News Agency. (2020). GCC Malware Analysis Platform Launched. https://www.bna.bh/en/GCCMalwareAnalysisPlatformlaunched.aspx?cms=q8FmFJgiscL2fwIzON1%2BDtn0tM2%2FwwMJUBiBhb5CV%2Fc%3D.

[12] National Information Security Center of the Sultanate of Oman. Objectives of the Information Security Ambassadors Program. https://ambassadors.cert.gov.om/about_ar.aspx.

[13] Cyberhub. https://cyberhub.sa.

[14] Saudi Federation for cybersecurity, programming & drones. Our initiatives. https://safcsp.org.sa/en/portfolio#section-HakathonHomthem.

[15] Coderhub. https://coderhub.sa.

[16] Tuwaiq Academy. https://tuwaiq.edu.sa.

[17] Bug Bounty. https://bugbounty.sa.

The status of Omani cybersecurity authorities is noteworthy: the Information Technology Authority, established in 2006, was transformed into the Ministry of Transportation, Communications and Information Technology in 2019[18]. Amman is also home to the Arab Region Innovation Center for Cybersecurity at the International Telecommunication Union (ITU-ARCC), which is managed by the National Center for Information Security[19]. Meanwhile, in the summer of 2023 the UN Office on Drugs and Crime's Regional Cybercrime Center was opened in Doha, Qatar.

The idea of creating cyber troops to fight terrorism in the Internet is being actively discussed. According to expert Abdullah Razzaq Al-Murjan, terrorist groups have changed their approach and moved to the strategy of "hidden unified supporters" (Arabic "المناصر المنفرد الخفي") in the virtual space. Back in September 2015, it was implemented in Kuwait established an electronic army after several serious cyberattacks (Albi I., 2017).

DISCUSSION AND CONCLUSION

First, although the concept of e-security, including criminal and criminological concepts, is not adopted by the highest authority in the GCC member states, it is represented in national strategies and policies in various fields, as well as in standards and guidelines. It is necessary to update national cybersecurity policies. Developing a local strategy is crucial (such as in the UAE and Dubai), since it allows to take into account the peculiarities of a particular state entity, given that it is one of the priorities of the national strategies of Oman and Bahrain. Moreover, it is vital to elaborate individual areas. For instance, on 14.06.2017, the Bahraini Information and E-Government Authority adopted the Cloud First Policy[20]. By 2021, more than 70% of the operations and systems of 72 government agencies have been migrated to the Cloud. The cost of improving technical infrastructure by 60-80% has been reduced. Building systems in the Cloud has helped the government overcome several challenges associated with

[18] Ministry of Transportation, Communications and Information Technology of the Sultanate of Oman. Information Technology Authority. https://www.ita.gov.om/ITAPortal_AR/Pages/Page.aspx?NID=2187&PID=6706&LID=247.

[19] ITU. Oman ITU-Arab Regional Cybersecurity Centre. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Partners/oman-itu-arab-regional-cybersecurity-centre.aspx.

[20] The Bahraini Information and E-Government Authority. Cloud First Policy. https://www.nea.gov.bh/Attachments/iGA_Cloud-First_Policy_V1.0.pdf

growing central infrastructure including human resources and costs, aligning government directives to reduce overall ICT expenditure and target expenditure, leveraging technological advances, meeting infrastructure development requirements due to lengthy traditional procurement procedures, increasing financial burden from infrastructure support, maintenance and management. Cloud computing has provided solutions to these problems by reducing costs, increasing simplicity, efficiency and quality of services, offering easy access to licenses and providing security systems in accordance with international standards. These advances have led to one of the largest cloud computing service providers in the world, Amazon Web Services Inc. choosing Bahrain as the location for its first data centers in the region, launching in 2019, helping to improve cyber resilience by leveraging advanced technologies[21].

Second, in GCC member states, the national cybersecurity centers (directorates) to which the CERTs report are independent central bodies in the field in question. Some of them have been transformed into separate ministries (as in Oman) or coexist with them because they have been reorganized from relevant commissions or committees (as in Qatar and KSA). The authorities are responsible for developing national strategies and implementing projects within the framework of governing documents, and may also include issues related to certification (UAE is an exception). There is a trend towards centralization of the bureaucracy. Within the structure of the Ministries of Interior, the police have established separate departments (directorates) to investigate electronic acts. Moreover, the system looks similar at the regional level within the Gulf Cooperation Council in terms of CERT, but not policies and institutions. The institutions vacillate between offensive and defensive strategies to combat electronic abuse.

Thirdly, the initiative of the UAE and Oman to establish e-ambassadors in different circles (academic, professional and layman) has several objectives: to increase the level of training of qualified personnel, their number, citizens' awareness of the issues, as well as the exchange of experience between specialists. In addition, the KSA has implemented the idea of hubs and boot camps for similar tasks, and Kuwait has implemented cyber troops. The initiatives considered can be mutually adopted at the national and regional levels.

[21] The Bahraini Information and E-Government Authority. Bahrain Government Has Successfully Adopted Cloud First Policy. https://www.iga.gov.bh/en/article/bahrain-government-has-successfully-adopted-cloud-first-policy#:~:text=Al%20Qaed%20said%20that%20the,Dr.

REFERENCES

Alkhaleej. First meeting of the Gulf Cybersecurity Committee in the UAE. https://alkhaleejonline.net/علوم-وتكنولوجيا/انعقاد-أول-اجتماع-للجنة-الخليجية-للأمن-السيبراني-بالإمارات.

Aljarida (2023). Gulf Cybersecurity recommends a unified strategy to combat cybercrime. https://www.aljarida.com/article/17840.

Alqurashi R. K., AlZain M. A., Soh B., Masud M., Al-Amri J. (2020). Cyber Attacks and Impacts: A Case Study in Saudi Arabia. *International Journal of Advanced Trends in Computer Science and Engineering*, 9 (1).

Alzubaidi A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, 7 (1), 1–13.

Communications, Space and Technology Commission. Cybersecurity in the telecommunications, space and technology sectors. https://www.cst.gov.sa/ar/RulesandSystems/CyberSecurity/Pages/default.aspx.

Communications, Space and Technology Commission. Maintaining the confidentiality of personal data. https://www.cst.gov.sa/ar/RulesandSystems/privacy/Pages/default.aspx.

General Secretariat of the Cooperation Council for the Arab States of the Persian Gulf. (2016). Electronic crime in the Gulf society and how to counter it. https://www.gcc-sg.org/ar-sa/CognitiveSources/DigitalLibrary/Lists/DigitalLibrary/البحوث%20الأمنية/كتاب%20الجريمة%20الالكترونية%20سلطنة%20عمان.pdf.

GCC General Secretariat. During the first meeting of the Ministerial Committee on Cybersecurity in the Gulf ... Launching the first Gulf cyber security exercise. https://www.gcc-sg.org/ar-sa/MediaCenter/NewsCooperation/News/Pages/news2022-10-23-4.aspx.

Albi I. (2017). Cyberwar. Here's how Gulf states are fighting terrorism electronically. https://alkhaleejonline.net/علوم-وتكنولوجيا/حرب-سيبرانية-هكذا-تكافح-دول-الخليج-الإرهاب-إلكترونياً.

KSA National Cybersecurity Authority. Controls and Guidelines. https://nca.gov.sa/legislation.

Ministry of Interior of the State of Qatar. Department of Combating Cybercrime. https://www.moi.gov.kw/main/sections/cyber-crime.

Ministry of Interior of the State of Qatar. General Directorate of Criminal Investigations.

https://portal.moi.gov.qa/wps/portal/MOIInternet/departmentcommittees/gacriminalinvestigation.

Mishaal Abdullah bin Hussein. Computer Incident Response Center Special Report on Information Technology Crimes 2008-2009. https://elaws.moj.gov.ae/UAE-MOJ_Fokeh/15_العدد%20الرابع/UAE-MOJ_2%تقرير%20مركز%20الإستجابة%20لطوارئ%20الحاسب%20الآلي%20لجرائم%20تقنية%20المعلومات0.html?val=UAE-FokehAA1.

Nir R., Clark R. (2011). Protecting e-Space in the Arab Gulf Cooperation Council Countries. Emirates Center for Strategic Studies and Research.

Oman News Agency Ministry of Technology and Communications participates in the meeting of the Executive Committee of e-Government and the Committee of Postal and Telecommunication Agencies in the Gulf States. https://omannews.gov.om/topics/ar/112/show/378724.

Salem F., Fiscbach T. (2017). *Cybercrime and the Digital Economy in the GCC Countries*. London: Chatham House.

Sherin O. (2013). Qatar’s National Cyber Drills. https://www.enisa.europa.eu/events/2nd-enisa-conference/presentations/Omar%20SHERIN-%20Q-CERT-%20Qatar%20-%202013%20CS%20drills%20for%20the%20Energy%20sector%20in%20Qatar.pdf.

Shestak V., Tsyplakova A. (2023). Countering Cyberattacks on the Energy Sector in the Russian Federation and the USA. *BRICS Law Journal*, 10(4), 35-52.

Shires J., Hassib B. (2022). Cybersecurity in the GCC: From Economic Development to Geopolitical Controversy. *Middle East Policy*, 29 (1), 90–103.

Seeger R. The New Battlefront: Cyber Security Across the GCC. https://gulfif.org/the-new-battlefront-cyber-security-across-the-gcc/.

Tsyplakova A.D. (2024). Theoretical and legislative characterization of cybercrime in Arab countries. Round table “Digital crimes: peculiarities of qualification”: Materials of I International Scientific and Practical Forum “The Law of Digital Security” (24-25 April 2024). Moscow: MGIMO University. https://ssrn.com/abstract=4822686.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET