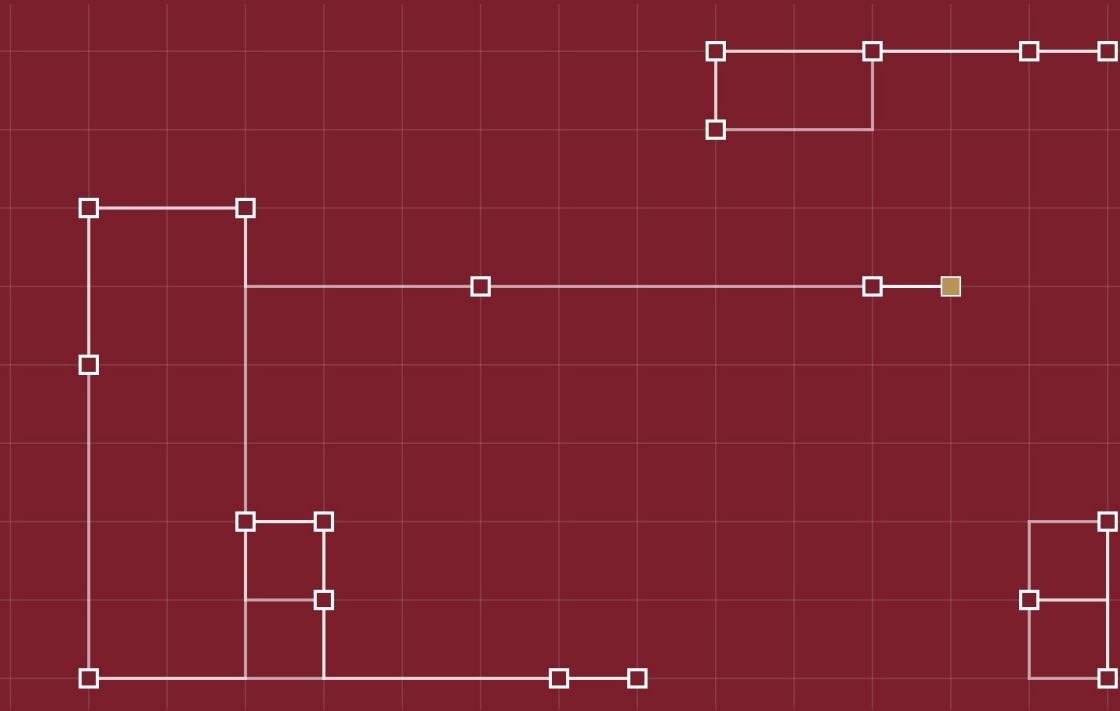


EPIC

Emirati Perspectives
and Insight Centre



POLICY PAPER • EPIC-PP-2026-026

Securing the Digital State

Cybersecurity Governance in the UAE

EPIC Research Team

October 2026

Securing the Digital State: Cybersecurity Governance in the UAE

Institutions, law and skills for a fully connected society under persistent attack

EPIC: Emirati Perspectives and Insight Centre

Abstract

In the United Arab Emirates, International Telecommunication Union (ITU) estimates published by the World Bank put internet use at 100 per cent of the population every year from 2020 to 2024. That level of connection makes cybersecurity a question of national resilience rather than a technical specialism. This paper examines how the UAE has organised its cyber defence since 2019, drawing on federal legislation, official strategy documents, statements by the UAE Cyber Security Council and ITU data. It finds that the institutional and legal framework has been built quickly and is rated highly: a national strategy was launched in 2019, a federal Cyber Security Council was created in November 2020, two federal decree-laws on cybercrime and personal data protection took effect on 2 January 2022, a new National Cybersecurity Strategy for 2025 to 2031 was approved in February 2025, and the UAE was placed in Tier 1, "role-modelling", of the ITU Global Cybersecurity Index 2024. The threat is persistent: in January 2025 the Council reported more than 200,000 attacks a day on strategic sectors. The paper identifies the main remaining gaps as the depth of the national cyber workforce, the absence of published national incident statistics over time, and the consistency of rules across federal, emirate and free-zone regulators. It closes with recommendations.

Keywords: UAE; cybersecurity; Cyber Security Council; National Cybersecurity Strategy; cybercrime law; personal data protection; Global Cybersecurity Index; critical infrastructure; cyber workforce; digital resilience

1. Introduction

Cybersecurity is the protection of networks, systems and data against attack, disruption and misuse. For a state whose government services, payments, logistics and utilities run on digital infrastructure, it is part of national security. This paper asks how the UAE has organised its cyber defence, how that organisation is assessed externally, and what gaps remain.

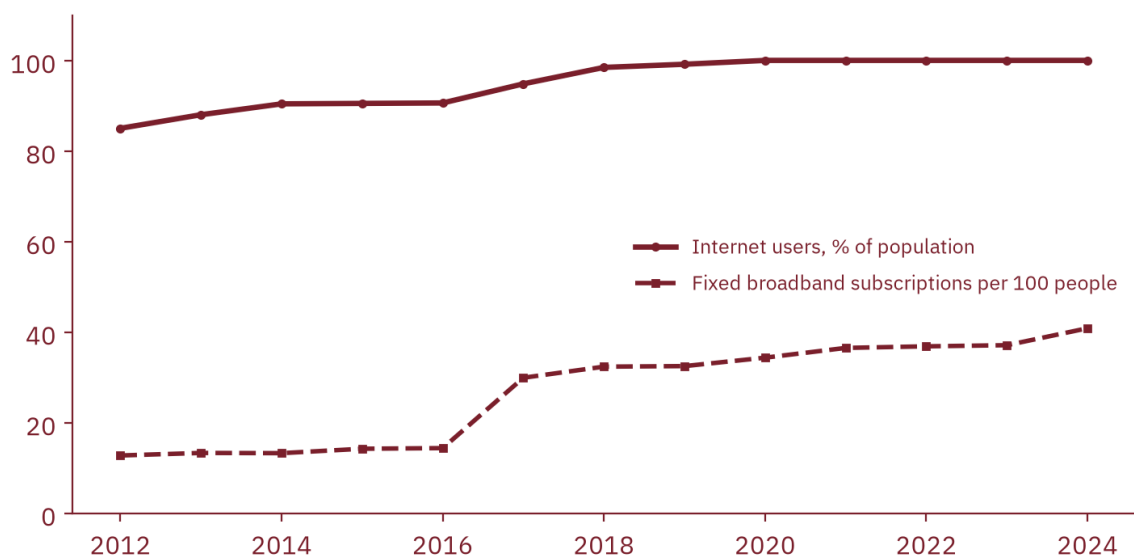
Section 2 sets out the exposure. Section 3 traces the institutions and strategies. Section 4 covers the legal framework. Section 5 reviews the threat as officially reported. Section 6 examines capability and skills, Section 7 identifies gaps, and Section 8 sets out recommendations.

2. A fully connected society

ITU estimates published by the World Bank show internet use in the UAE rising from 85 per cent of the population in 2012 to 100 per cent from 2020 onwards (Figure 1). Fixed broadband subscriptions rose from about 13 to about 41 per 100 people between 2012 and 2024, and mobile subscriptions stood at about 203 per 100 people in 2024. Secure internet servers, a rough indicator of the volume of encrypted online services hosted in the country, rose from about 293 per million people in 2012 to about 4,192 in 2024, although the series is volatile from year to year.

High connectivity is an economic asset and a source of exposure. Every additional digital service enlarges what an attacker can target.

Figure 1. Internet use and fixed broadband, UAE, 2012–2024



Source: World Bank, WDI (ITU data): IT.NET.USER.ZS, IT.NET.BBND.P2, retrieved 25 Oct 2026
Chart: EPIC: Emirati Perspectives and Insight Centre

3. Institutions and strategy

The UAE's first comprehensive strategy of the current period was the National Cybersecurity Strategy launched in June 2019 by the telecommunications regulator, then the Telecommunications Regulatory Authority and now the Telecommunications and Digital Government Regulatory Authority (TDRA). It was built on five pillars and 60 initiatives, set a goal of developing the capabilities of more than 40,000 cybersecurity professionals, and was to remain in force for three years. In January 2020 the regulator launched a National Cybersecurity Capacity Building Programme under the strategy.

In November 2020 the UAE Cabinet agreed to establish the UAE Cyber Security Council, chaired by the Head of Cyber Security for the UAE Government. Its mandate covers a comprehensive cybersecurity strategy, a legal and regulatory framework covering all types of

cybercrime, the security of existing and emerging technologies, and a National Cyber Incident Response Plan.

In February 2025 the Cabinet approved a new National Cybersecurity Strategy, published by the Council as the strategy for 2025 to 2031. It has five pillars: governance, protection, innovation, development of national digital and cyber capabilities, and partnership. Figure 2 sets out the sequence.

Figure 2. Milestones in UAE cybersecurity governance, 2019–2025



Source: u.ae; TDRA (21 Jan 2020); WAM (29 Nov 2020); UAE Legislation (FDL 34/2021, FDL 45/2021); ITU (10 Sep 2024); UAE Cabinet (Feb 2025)
Chart: EPIC: Emirati Perspectives and Insight Centre

4. The legal framework

Two federal decree-laws that took effect on 2 January 2022 form the core of the legal framework.

Federal Decree-Law No. 34 of 2021 on Countering Rumours and Cybercrimes was issued on 20 September 2021. The official UAE portal describes it as a comprehensive framework to address the misuse and abuse of online technologies.

Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data applies to the electronic processing of personal data inside or outside the country. It prohibits processing without the consent of the data subject except in listed cases, sets controls on processing, gives individuals rights to correction and restriction, and sets requirements for cross-border transfer. The official portal notes that it was the first federal law drafted in partnership with major private-sector technology companies.

Sector laws add to this, including Federal Law No. 2 of 2019 on the use of information and communication technology in health fields.

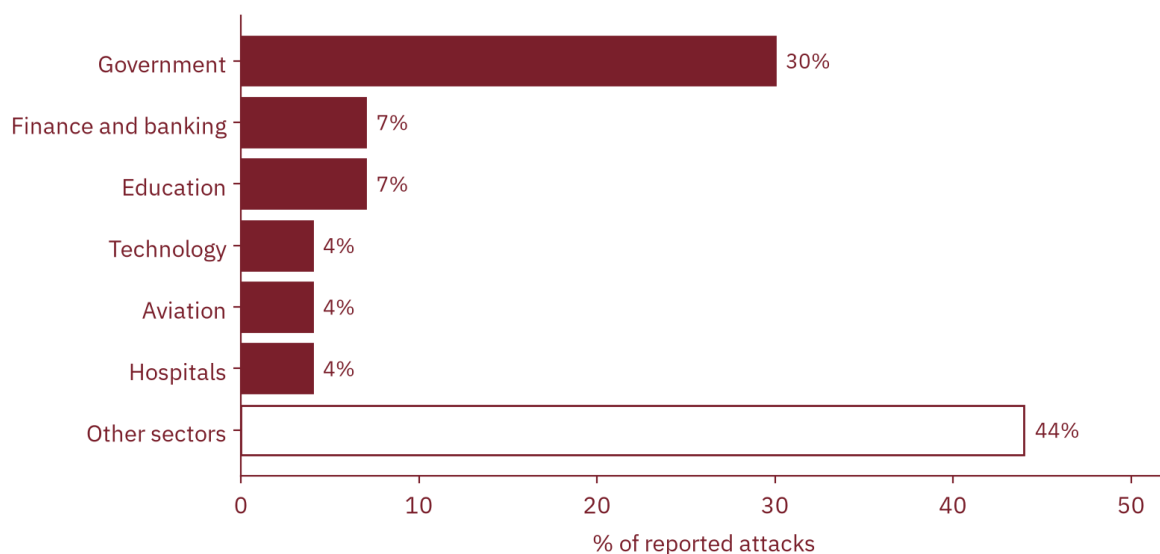
5. The threat as officially reported

The UAE Cyber Security Council publishes threat information episodically rather than as a regular statistical series. In February 2024 it reported that national systems had repelled cyberattacks by terrorist organisations against vital and strategic sectors. In October 2024 its chairman said that the UAE had once detected more than 200,000 attacks in a single week during a period of regional geopolitical tension, none of which harmed systems.

In January 2025 the Council reported that attacks on strategic sectors had exceeded 200,000 a day, originating from groups in 14 countries. By its account, government was the most targeted sector at 30 per cent of attacks, followed by finance and banking and education at 7 per cent each, and technology, aviation and hospitals at 4 per cent each (Figure 3). The most frequent incident types were incorrect configurations (27 per cent), malware (22 per cent), scanning and login attempts (15 per cent) and unauthorised access (15 per cent).

These figures come from a single official source and use the Council's own definitions. They cannot be compared reliably over time or with other countries.

Figure 3. Reported attacks on strategic sectors by target, UAE, Jan 2025



Source: UAE Cyber Security Council (via WAM), 20 Jan 2025: share of cyberterrorist attacks on strategic sectors by target sector
Chart: EPIC: Emirati Perspectives and Insight Centre

6. External assessment and capability

The ITU Global Cybersecurity Index 2024 assessed countries on five pillars: legal, technical, organisational, capacity development and cooperation. It placed the UAE in Tier 1, "role-modelling", the highest of five tiers, reserved for overall scores of 95 to 100. Tier 1 contained 46 countries. The 2024 edition reports tiers rather than ranks, so it does not support claims about the UAE's position relative to other Tier 1 countries.

On skills, the April 2025 agreement between the Council and Google Cloud provides for a cybersecurity centre of excellence in Abu Dhabi, with training delivered by Google's Mandiant

unit. Research by Access Partnership cited in the announcement projected that stronger cyber capabilities could support over 20,300 specialised cybersecurity jobs by 2030. This is a projection commissioned in connection with a commercial partnership, not an official workforce estimate.

7. Gaps

Workforce. The 2019 strategy aimed to develop more than 40,000 cybersecurity professionals. No official figure was found on how many have been trained or how many cybersecurity professionals work in the UAE, so progress against that goal cannot be assessed.

Incident statistics. Threat data are released as occasional announcements with changing definitions. Without a regular national series of reported incidents, breaches and losses, it is difficult to judge whether resilience is improving.

Regulatory consistency. Cyber and data rules are set by federal bodies, emirate-level authorities and free zones with their own regimes. The 2025 to 2031 strategy places governance first among its pillars, which indicates that coherence is recognised as a priority.

Monetary losses. No official estimate of losses from cybercrime in the UAE was found.

8. Recommendations

1. **Publish an annual national cyber incident report.** Use stable definitions for incidents, sectors and severity so that trends can be tracked.
2. **Set and report a workforce baseline.** Publish the number of certified cybersecurity professionals and track it against national targets.
3. **Align rules across regulators.** Use the governance pillar of the 2025 to 2031 strategy to establish a common baseline standard that applies across federal, emirate and free-zone regimes.
4. **Report on the National Cyber Incident Response Plan.** Publish summary results of national exercises, including those involving critical infrastructure operators.
5. **Evaluate partnerships.** Report outcomes of training partnerships with private companies in terms of graduates and placements, not only announcements.

9. Conclusion

In six years the UAE has built a national cyber security institution, a modern legal framework for cybercrime and personal data, and two national strategies, and has earned the top tier of the ITU index. The next test is measurement: showing, through regular public data, that the workforce is growing and that incidents are being contained.

About this paper

This paper was prepared by the EPIC Research Team as part of the daily papers programme. All figures were verified against the sources listed below on 25 October 2026. Claims that could not be verified were removed. See the accompanying sources and verification notes.

References

Access Partnership, cited in Google Cloud. 2025. "Empowering Cyber Defense: UAE and Google Cloud to Collaborate on Cybersecurity." Press release, 9 April 2025. <https://www.googlecloudpresscorner.com/2025-04-09-Empowering-Cyber-Defense-UAE-and-Google-Cloud-to-Collaborate-on-Cybersecurity>.

International Telecommunication Union. 2024. *Global Cybersecurity Index 2024*. Geneva: ITU. <https://www.itu.int/epublications/publication/global-cybersecurity-index-2024>.

International Telecommunication Union. 2024. "Global Cybersecurity Index 2024." Press release, 10 September 2024. <https://www.itu.int/en/mediacentre/Pages/PR-2024-09-10-Global-Cybersecurity-Index.aspx>.

Khaleej Times. 2024. "UAE blocks 200,000 cyberattacks in one week amid geopolitical issues: Top official." 17 October 2024. <https://www.khaleejtimes.com/business/tech/uae-blocks-200000-cyberattacks-in-one-week-amid-geopolitical-issues-top-official>.

TDRA. 2020. "TRA launches the National Cybersecurity Capacity Building Program." 21 January 2020. <https://tdra.gov.ae/en/media/press-release/2020/tra-launches-the-national-cybersecurity-capacity-building-program>.

UAE Cabinet. 2025. "UAE Cabinet approves National Cybersecurity Strategy, API-First Policy." February 2025. <https://uaecabinet.ae/en/news/uae-cabinet-approves-national-cybersecurity-strategy-api-first-policy>.

UAE Cyber Security Council. 2025. "CSC Announces Countering 200,000 Cyberattacks Daily from Terrorist Groups Across 14 Countries." 20 January 2025. <https://csc.gov.ae/en/w/csc-announces-countering-200-000-cyberattacks-daily-from-terrorist-groups-across-14-countries>.

UAE Cyber Security Council. n.d. "Discover CSC" and National Cybersecurity Strategy 2025 to 2031. <https://csc.gov.ae/en/discover-csc>.

UAE Government Portal. n.d. "National Cybersecurity Strategy 2019." <https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/strategies-plans-and-visions-untill-2021/national-cybersecurity-strategy-2019>.

UAE Government Portal. n.d. "UAE Cybersecurity Council." <https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/uae-cybersecurity-council>.

UAE Government Portal. n.d. "Data protection laws." <https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws>.

UAE Legislation. 2021. Federal Decree-Law No. 34 of 2021 on Countering Rumours and Cybercrimes. <https://uaelegislation.gov.ae/en/legislations/1526>.

UAE Legislation. 2021. Federal Decree-Law No. 45 of 2021 Concerning the Protection of Personal Data. <https://www.uaelegislation.gov.ae/en/legislations/1972>.

WAM. 2020. "Mohammed bin Rashid approves UAE Environment Policy, UAE Cybersecurity Council and UAE National Media Team." 29 November 2020. <https://www.wam.ae/en/article/hszrbd77-mohammed-bin-rashid-approves-uae-environment>.

WAM. 2024. "National systems foil attempted cyberattacks by terrorist groups: UAE Cyber Security Council." 9 February 2024. <https://www.wam.ae/en/article/b1kt3yi-national-systems-foil-attempted-cyberattacks>.

WAM. 2025. "UAE to launch National Cybersecurity Strategy." 11 February 2025. <https://www.wam.ae/en/article/bi5dfsr-uae-launch-national-cybersecurity-strategy>.

World Bank. 2026. World Development Indicators: IT.NET.USER.ZS, IT.NET.BBND.P2, IT.CEL.SETS.P2, IT.NET.SECR.P6 (ITU and Netcraft data). Retrieved 25 October 2026. <https://data.worldbank.org>.