13. The United Arab Emirates

The recognition by the UAE of cyberspace as a critical foundation of economic growth and diversification away from oil dependence has led it to develop comprehensive policies to improve national cyber resilience. However, the country also views cyberspace as a threat to political stability and it invests heavily in cyber surveillance of its population, including guest workers. The UAE's national cyber-security governance rests on a centralised framework where federal authorities act under the direction of the Supreme Council for National Security. While the UAE is committed to building up its cyber-intelligence assets, it largely relies on technology transfer or foreign procurement for access to sophisticated cyber tools. The digital economy remains heavily dependent on Western expertise for the most advanced technologies. The UAE's overall cyber-security posture has improved in the past decade through regulatory means and partnerships with foreign industry players, but it still lacks the ability to coordinate a comprehensive response in the case of a national cyber emergency. The UAE's diplomatic engagement in global cyber governance has also been limited, focused largely on retaining sovereignty over its cyberspace. To manage internal security and advance foreign-policy objectives, the UAE has shown a willingness to use offensive cyber tools, most often procured from foreign entities. We assess the UAE to be a Tier-Three cyber power primarily due to limitations in scale and reliance on foreign capabilities for cyber technologies.

Strategy and Doctrine

Ensuring a secure national ICT infrastructure and cyberspace is critical to many of the UAE's digital strategies as the country seeks to diversify the economy away from oil. At the 2022 International Defence Industry Technology and Security Conference, the UAE's top cyber-security official emphasised that security is the 'integral pillar‘ of national digital-transformation efforts, highlighting recognition at the high echelons of government that cyber security is foundational to national security and prosperity.[1]

Dubai stands out among the seven emirates of the UAE in its ambition to exploit and secure the cyber domain.[2] The first document on cyber strategy in the UAE was published by the Dubai Electronic Security Center (DESC) in 2017, and it was specific to the emirate.[3] The DESC was established in 2014 to 'ensure that Dubai becomes a leader in cyber security and the protection of information from external cyber threats'.[4] The Dubai Cyber Security Strategy aimed at making Dubai among the most electronically secure cities in the world. It also aimed to ensure cyber resilience and promote cyberspace innovation, as well as growth and economic prosperity in the emirate. The strategy provisions were civilian and defensive with a focus on five priorities:

List of Acronyms

aeCERT	National Computer Emergency Response Team
CPX	Cyber Protection X Holdings
CSC	Cyber Security Council
DESC	Dubai Electronic Security Center
FTTH	Fibre to the home
IAR	Information Assurance Regulation
ISNR	International Exhibition for National Security and Resilience
NCSS	National Cyber Security Strategy
NESA	National Electronic Security Agency
SCNS	Supreme Council for National Security
SIA	Signals Intelligence Agency
TDRA	Telecommunications and Digital Government Regulatory Authority

- a cyber-smart society: increasing public awareness and developing cyber skills and capabilities in private and public institutions as well as by individuals
- innovation: conducting R&D in the field of cyber security
- cyber security: establishing controls to safeguard the confidentiality, credibility, availability and privacy of data
- cyber resilience: ensuring the continuity and availability of IT systems in the face of cyber incidents
- national and international collaboration in cyber security: strengthening cooperation between different sectors and actors at the local and global levels

A country-wide cyber-security strategy followed in 2019. The National Cyber Security Strategy (NCSS) was published by the Telecommunications and Digital Government Regulatory Authority (TDRA) and was planned to be in force until June 2022, though no updated strategy had been released as of early June 2023.[5] The NCSS targeted five priorities:

- laws and regulations governing cyber crimes and securing existing and emerging technologies
- a vibrant security ecosystem using the local security market while tapping the larger regional market, as well as training over 40,000 cyber-security professionals and supporting cutting-edge research and innovation
- a national incident-response plan enacting quick and coordinated reaction to cyber incidents; measures including streamlining detection and reporting of security incidents and establishing a common severity-assessment matrix
- the Critical Information Infrastructure Protection Policy focusing on protecting critical sectors including energy, emergency services, finance, health services, ICT and transportation
- partnerships mobilising security and comprising the public and private sectors, academia and international consortiums

Indeed, at a recent cyber-security and innovation conference, the UAE's Head of Cyber Security emphasised that partnerships with 'like-minded' countries and entities is the 'first line of defence' against cyber threats.[6] The UAE government understands that collaborating with a broad spectrum of partners is key to elevate domestic cyber-security capabilities. Besides the United States, a close security and defence partner, the UAE also has joint initiatives with Israeli and Chinese industry leaders to develop cyber technologies.[7]

The UAE military likely possesses cyber capabilities and will continue to develop capacity and concepts to integrate them more fully into their existing and future force architectures. The International Defence Conference in February 2021 in Abu Dhabi, organised in collaboration with the Ministry of Defence and the General Command of the UAE Armed Forces, showed areas of focus in cyber security, R&D, supply chain and artificial-intelligence protection.[8] While this illustrates that the armed forces are clearly aware of the potential of cyberspace, little public information about the UAE's military strategy or doctrine in cyberspace is available.

The UAE has effectively engaged in mass surveillance of its population through cyber means to ensure political stability. Its wide-ranging methods include using relatively affordable botnets on social-media platforms to shape public narratives, controlling national telecommunications companies to monitor internet traffic and enforce censorship as well as procuring sophisticated surveillance infrastructure from foreign vendors.[9] A business partnership involving Israeli and UAE entities reportedly built a country-wide surveillance platform dubbed *Falcon Eye* that can integrate sensors across crucial city functions into one command-and-control system.[10] Authorities like the TDRA have also publicly acknowledged the government's ability to track social media and internet sites.[11]

Overall, the UAE uses a multipronged approach to national cyber security: protecting critical information infrastructure; developing cyber legislation; investing in local cyber-security expertise; and comprehensive surveillance of domestic political activism.

Governance, Command and Control

The UAE's cyber-governance structure begins at the highest level with the Supreme Council for National Security

(SCNS) headed by the President Sheikh Mohammed bin Zayed al-Nahyan. The Head of Cyber Security acts as executive advisor to the council.[12] Given the immense weight and reach of the council, cyber security is coordinated at the highest echelons of the government.

In November 2020, the UAE cabinet approved the establishment of the UAE Cyber Security Council (CSC), which is chaired by the Head of Cyber Security. The council met for the first time in January 2021 and was instrumental in setting new cyber-security standards for government agencies announced in October 2021.[13] The CSC is responsible for various aspects of national cyber security, including updating its strategy, establishing a national incident-response plan as well as developing legislation and policies for strengthening security across all sectors in the UAE.[14]

Before the CSC was established, the National Electronic Security Agency (NESA) was responsible for the development and implementation of cyber-security strategies, policies and standards in the UAE.[15] It still retains parts of that role. Established in August 2012 under the umbrella of the SCNS after the Arab Spring, NESA directly reported to the country's then-national security advisor.[16] To mitigate perceived threats against the regime, NESA was involved in hacking and interception activities using spyware procured from private commercial firms.[17] In September 2018, NESA remained in existence but was reorganised into three entities, the largest of which was the new Signals Intelligence Agency (SIA).[18] The SIA retains hacking capabilities and remains under the umbrella of the national-security establishment, notably the SCNS.

The UAE Cyber Security Council first met in 2021

The TDRA is another important player, as it is responsible for enforcing many of the rules and regulations in the ICT sector and managing the overall digital infrastructure in the UAE.[19] Data flowing through the country's networks are required to be filtered and shared with relevant state authorities. Notable content filtering takes place on matters concerning the state, foreign policy and morality issues, but details on specific content-filtering rules are not publicly available.

The UAE's cyber capabilities are dispersed over several entities among the emirates. For instance, the Abu Dhabi Digital Authority, Dubai Digital Authority and Department of Digital Ajman have incorporated cyber security in their goals of digital transformation.[20] While unified in the mission to protect state security with all means possible, differences in priorities exist and they often stem from a trade-off between economic and security priorities. The spread of cyber-security and surveillance capabilities across multiple federal entities also serves to ensure a pervasive counter-intelligence capability throughout the system to strengthen regime security.[21] Nevertheless, it is unclear how well these emirate-level authorities interact with the TDRA on the federal level and collaborate among one another on the inter-emirate level.[22]

Regarding military cyber organisation, the UAE Armed Forces reportedly launched a cyber command within its General Headquarters.[23] However, there has been no publicly available evidence of the command's cyber capabilities. In addition, while there is a clear distinction as to roles and responsibilities between defence intelligence and general intelligence, many officials on the civilian side are being recruited through the military, which has led to strong operational links.

Overall, the UAE's national cyber-infrastructure governance rests on an increasingly centralised framework where federal authorities such as the CSC, SIA and TDRA act under the direction of the SCNS. Federal guidelines and frameworks also aim to enable coordination among the various cyber authorities at the emirate level.

Core Cyber-intelligence Capabilities

The security industry is one of the largest sectors in the UAE, as the federal government is eager to position itself at the forefront of developing and adopting the latest surveillance technologies. Due to the UAE's financial clout, the centralised power of its state authorities as well as the small size of the country and population, cutting-edge surveillance technologies and capabilities can be quickly deployed. The UAE's high-tech security camera networks, sensors and tracking tools are increasingly integrated. Authorities can generate comprehensive electronic profiles of all individuals in the country. The Ministry of Interior and security services are prominent players tasked with ensuring domestic security and resilience, including the use of cyber capabilities to support national-security objectives. These 'defensive' capabilities work in conjunction with stringent cyber-security laws.[24]

The UAE's cyber-intelligence capabilities rely heavily on semi-private companies. Due to a lack of local expertise and strategic planning, the SIA and its predecessors have been greatly dependent on foreign cooperation and expatriates with an intelligence background, in particular from the US, the United Kingdom and more recently Israel.[25] For instance, US defence group Raytheon aided in the founding of NESA by integrating the agency's infrastructure networs. Raytheon subcontracted much of the work to other US technology vendors including Cisco and Booz Allen Hamilton.[26] The UAE government also established local entity DarkMatter[27] as a preferred partner for NESA, involving the recruitment of ex-US National Security Agency hackers and Israeli elite cyber-security personnel.[28] Following an exposé of DarkMatter's hacking activities,[29] the company was reorganised to focus only on defensive cyber activities. Former hacking roles within DarkMatter were transferred to semi-public UAE companies such as BeamTrail and Protect Electronic.[30] These companies were later incorporated into EDGE Group, a government-led defence conglomerate. It was established in November 2019 and has rapidly become the preferred vehicle for developing intelligence and security technologies.[31] EDGE's hybrid-warfare subsidiary Beacon Red also has a cyber focus.[32] It is in turn a rival of Cyber Protection X Holdings (CPX), created in March 2022 under state-owned AI entity Group 42 to control the UAE's cyber-intrusion capabilities.[33] Despite internal power struggles, the control of the entire cyber-intelligence sector is ultimately centralised under the National Security Advisor.

Media reports have also accused the UAE of purchasing and using malware designed for tracking and intimidating political dissidents.[34] For instance, Reuters ran a special report on *Project Raven*, where Abu Dhabi targeted its residents and citizens.[35] Moreover, the Emirati government reportedly spent millions of dollars on malware to conduct electronic surveillance of dissidents and political opponents.[36]

While the UAE has ambitions to develop sovereign cyber-intelligence technologies, the authorities still rely on purchasing technologies and learning from technology transfers from foreign firms. It has done so with the Italian firm Hacking Team (now defunct) and Israeli company NSO Group.[37] The establishment of diplomatic relations with Israel through the Abraham Accords of September 2020 has boosted the UAE's cyber-intelligence capabilities through open partnerships and investments from Israeli cyber firms.[38]

Overall, the UAE has significant domestically focused cyber-intelligence capabilities and some limited regional reach.

Cyber Empowerment and Dependence

Cyberspace plays an important role in Abu Dhabi's efforts to diversify its economy away from oil. Since the early 2000s, the UAE has set ambitious goals in digital innovation and e-governance.[39] The COVID-19 pandemic prompted the publication of the UAE Strategy for Government Services and the National Digital Government Strategy 2025 to improve digital government services.[40] By law, every UAE resident carries an electronic identity card which bears the holder's biometric details and is essential for a wide range of government services.[41] Underscoring the deep appreciation of digitalisation to transform the UAE's development for the long term, digital excellence was included in the 'Ten Principles' adopted in 2021 to guide development over the next 50 years.[42] Accompanying the ten principles are the 'Projects of the 50', where digitalisation, advanced technologies and cyber-related initiatives feature prominently alongside other flagship projects.[43] The government has also released several initiatives at the national and local levels to spur ICT innovation and digital transformation of strategic sectors.[44] As of April 2022, the digital economy contributed 9.7% to the UAE's GDP. The Digital Economy Strategy indicates the government's aims to double digital economy contribution to 19.4% within ten years.[45]

The UAE population is highly dependent on digital services. The country has scored well in critical indicators such as smartphone penetration,[46] smart-city platforms[47] and e-government services.[48] The UAE has maintained the world's highest penetration of fibre to the home (FTTH) since 2016, according to industry body FTTH Council in 2022.[49] At the start of 2022, internet penetration stood at an impressive 99%.[50] Robust ICT infrastructure partly contributed to the UAE's strong rankings in the Portulans Institute Network Readiness Index 2022, which placed it 28th globally, ahead of Saudi Arabia (35th) and Qatar (42nd).[51] The UAE's strengths were also reflected in investment in emerging technologies (10th), gross expenditure on R&D financed by business (5th) and government online services (15th). The index also indicated UAE weaknesses in e-commerce legislation (87th) and its ICT regulatory environment (74th).

The Emirates has significant control over its telecommunications infrastructure. Etisalat UAE and Du are the two most dominant telecommunications providers by market share in the country. They are majority state-owned, though both companies have announced plans to increase foreign shareholding limits from 20% to 49% in a bid to increase foreign direct investment.[52] Like Saudi Arabia, the UAE diversifies its wireless equipment and services vendors to avoid reliance on a single vendor. Nokia, Huawei and Ericsson have all partnered with the UAE to deploy 5G networks.[53]

The UAE wants to be seen as a pioneer of disruptive technologies, digital innovation as well as cyber and space capabilities. Abu Dhabi appointed in 2019 an ambassador for the Fourth Industrial Revolution and introduced the Ministry of Industry and Advanced Technology in a 2020 government reshuffle. In addition, the UAE established an Advanced Technology Research Council in 2020. The Emirates are also striving to be a tech-startup hub by launching the National Program for Coders that offers 'golden visas' to coders and companies specialising in coding.[54] In October 2021, the UAE set the objective of having the highest per capita number of female coders worldwide in the next decade.[55]

Like Saudi Arabia, the UAE places importance on developing artificial intelligence. In 2017, the government appointed a minister for AI and issued a national strategy with the aim of becoming a leading AI power by 2031.[56] The Mohamed bin Zayed University of Artificial Intelligence, established in 2019 as the world's first AI university, was ranked 30th in AI research among other globally renowned research universities by CSRankings, a ranking of top computer science institutions worldwide.[57] Among 2022 rankings of publications in the two most prestigious AI-research conferences, the UAE was 27th among the top 50 countries leading in AI research, second behind Saudi Arabia (18th) among the Arab states.[58] Within the domestic defence industry, EDGE is trying to develop a niche in autonomous capabilities and AI,[59] while Group 42 is strengthening geospatial intelligence capabilities through cooperation with US partners.[60]

Within the space sector, the UAE's state-owned satellite provider – Al Yah Satellite Communications Company PJSC (Yahsat) – ranks among the top-ten satellite operators by revenue globally. Established in 2007, it has provided a broad range of fixed and mobile satellite services spanning voice and data communications in more than 150 countries.[61] The UAE military relies on satellite communications provided by Yahsat and its Thuraya subsidiary.[62] Yahsat is expected to launch the Thuraya 4 Next Generation satellite in 2023, which would improve capacity and coverage across various continents for defence, governmental and commercial purposes.[63] The UAE has some way to go before it achieves autonomy in the space sector. The country relied on foreign expertise to build the Thuraya 4 satellite,[64] which is expected to be launched by SpaceX, a US spacecraft manufacturer.

The UAE is also trying to build an international profile as a producer of security and defence capabilities. It has already achieved some degree of success in this regard. For example, EDGE Group ranked among the top 25 military suppliers in 2020 according to the Stockholm International Peace Research Institute – the first Arab firm to do so.[65] EDGE aims to make the UAE a global player in advanced technology, particularly in addressing hybrid threats, by streamlining the local defence industry and reducing foreign dependence. In June 2022, EDGE signed an agreement which would see it expand global exports of more than 40 domestically manufactured products.[66] The Emirati government has also consistently invested in technology innovation.[67] However, most of its equipment exports have been low-tech, and the UAE remains reliant on foreign partnerships and technology transfers for the most advanced equipment.

The UAE government has embraced digitalisation through dedicated policies and investments. This is largely manifested in the country's strong ICT infrastructure and e-governance system. While the Emirates has also achieved marked progress in developing a sovereign space and defence industry, it still relies on US and other Western entities for expertise in advanced technologies.

Cyber Security and Resilience

Besides being a hotspot for attack by cyber criminals, the UAE is a constant target of sophisticated state actors for political and economic purposes. A threat assessment of attacks in the commercial sector in 2021 indicated that UAE organisations were each targeted an average of 295 times per week. Organisations in the finance and banking sectors recorded the highest average number of weekly attacks at 407.[68] By 2023, the number of attacks was being counted at 50,000 per day.[69] In response, the UAE has made significant strides towards ensuring the monitoring, detection and protection of its critical infrastructure. In March 2023, a senior official said that ransomware attacks in the country had declined more than 70% since the start of the year, following a 14% drop in malware in 2022.[70]

Cyber-security regulations in the UAE are regularly updated to counter these threats. The 2021 Law on Combatting Rumours and Cybercrimes (Cybercrimes Law) as well as the Information Assurance Regulation (IAR) are amongst the most important cyber-security laws and regulations. The 2021 Cybercrimes Law updated the 2012 version and covers offences for sectors such as banking, media, health and scientific institutions. It also emphasises content-related offences regarding misinformation, including on social media.[71] The IAR replaced the Information Assurance Standards in March 2020.[72] The TDRA developed the IAR, which aims at raising the minimum level of cyber security across the Emirates at the national, sector and entity levels. Compliance is mandatory for all government agencies and entities designated as critical information infrastructure.[73] The IAR builds on the National Cyber Risk Management Framework, which defines the NESA risk-assessment process. In October 2021, new cyber-security standards for government agencies the CSC proposed were also approved.[74]

The UAE's ability to coordinate a whole-of-nation response to significant cyber incidents is still under development, but notable progress has been achieved. The CSC in 2021 reported discussions on mechanisms to contain cyber emergencies as well as progress in developing a national incident response plan.[75] More recently, the council entered into a strategic partnership with CPX, which will assist in standardising the country's national cyber-security operations, build technical and operational capabilities for responding to cyber incidents as well as develop nationwide cyber skills.[76] The National Computer Emergency Response Team (aeCERT), operating under the TDRA, disseminates information during a significant cyber attack and handles communication with national and international authorities in response efforts.[77] By 2023, NESA has issued a comprehensive policy on protection of critical information infrastructure.[78] The same year, the UAE broke with diplomatic precedent and established a new multinational cyber-security system involving Israel, citing the principle that unified efforts were essential to counter the escalating threats.[79] Dubbed *Crystal Ball*, the project will create a situational-awareness platform based on cross-border collaboration intended to 'design, deploy and enable regional intelligence enhancement'.

A government centre manages all security events round the clock in FedNet, a secure network architecture for all federal government entities.[80] According to the UAE's Head of Cyber Security, there is full coordination between federal and local departments on dealing with cyber threats, and cyber exercises are conducted involving government agencies and cyber-security stakeholders.[81] In addition, the UAE's National Emergency Crisis and Disasters Management Authority is mandated with raising readiness and resilience of institutions and society when confronted with risks, including cyber attacks. Among other things, it provides business-continuity management guidelines in case of attacks.

Measures to improve resilience in the finance sector have also taken effect. In January 2020, for example, the

Dubai Financial Services Authority launched a Cyber Threat Intelligence Platform as part of efforts to improve cyber security within the Dubai International Financial Centre.[82] The initiative was set up in collaboration with the DESC and aeCERT. In November 2021, the Central Bank of the UAE announced the establishment of its Networking and Cyber Security Operations Centre to better secure the nation's financial information infrastructure against cyber attacks.[83] Cyber security of the nuclear-power sector is another very high priority for the UAE, with the nuclear authority laying out stringent regulations for the operator.[84]

To overcome the lack of expertise in cyber-security technology, the CSC has set up partnerships with established foreign players such as Amazon Web Services, Deloitte and Huawei.[85] The partnership with Amazon deals with cloud cyber security, while the partnership with Deloitte aims to bolster the UAE's cyber capabilities through training, implementation of cyber security as well as introduction of global best practices. What is more, Huawei formed an independent think tank with CSC focusing on cyber-security research. Group 42 also engaged Palo Alto Networks for automated protection of its network systems.[86] In addition to foreign partners, the CSC signed a memorandum of understanding with CPX and Injazat to improve the cyber security of government and semi-government entities.[87] Besides improving national cyber resilience, these partnerships aim to develop the security industry as a robust and sustainable sector of UAE's national economy.

The Emirati government has also invested in initiatives to boost the local cyber workforce. It developed a national awards programme to support security research and start-ups.[88] The Cyber Node initiative the DESC launched in partnership with France's Thales Group aims to convene cyber experts from the public and private sectors and academic institutions and provide an environment for improving workforce skills.[89] The CSC launched the National Bug Bounty Programme in 2021 to promote cyber-security culture and engage local talent.[90]

Overall, the UAE's efforts to improve its cyber security have reaped notable results. Its position in the UN International Telecommunication Union Global Cybersecurity Index improved from 33rd in 2019 to fifth in 2020.[91] The UAE's cyber-security industry is nascent, but is poised for strong growth given extensive partnerships established with foreign industry players.

Global Leadership in Cyberspace Affairs

The UAE's engagement in cyber diplomacy largely emphasises its stance on maintaining cyberspace sovereignty. It retains a strong alliance with the US while building up cyber-security partnerships with countries such as Israel and the UK. The UAE seeks to carve out a position of global leadership in digital innovation, space and security technology.

Playing into its advantage of location and air connections, the UAE hosts various regional and global conferences on cyber and information security. Dubai, for example, hosts the Gulf Information Security Expo and Conference, which is the largest cyber-security conference in the region. It also hosts GITEX, a major tech show, and the relatively new Cybertec conference. In addition, during the 2022 World Government Summit in Dubai, the International Civil Aviation Organization signed a new partnership with the UAE to improve aviation cyber security in the Middle East.[92] Abu Dhabi hosts the International Exhibition for National Security and Resilience (ISNR), which showcases the latest innovations in the security sector. Central themes of ISNR 2022 included cyber security, policing and law enforcement as well as critical-infrastructure protection with a focus on new technologies and best practices.[93]

The UAE tends to follow Russian and Chinese views on international attempts to regulate cyberspace. The Gulf state voted in favour of two Russian-sponsored resolutions, one on cyber governance and one on cyber crime, in the UN General Assembly in December 2018.[94] The Emirates also voted in favour of a Russian resolution, which envisioned a committee on a new UN cyber-crime treaty, in December 2019.[95] 'Our borders in cyberspace are sovereign borders that we always need to protect and consolidate their defences,'[96] UAE Prime Minister and Dubai Ruler Sheikh Mohammed bin Rashid said in October 2021.

In sum, the UAE has been highly engaged in hosting international conferences and supporting entrepreneurship regarding technological innovation and defence technology as it seeks to portray itself internationally as a leading nation in these fields. It is more reserved in its engagement regarding global cyber-affairs governance. The Emirates falls in the camp of advocates of cyber sovereignty and sees cyberspace more as a national rather than an international area for rules and regulations.

Offensive Cyber Capability

The UAE sees offensive cyber assets as part of its toolbox to advance foreign-policy goals, but there is only occasional and limited reporting on such operations by it. In 2017, Abu Dhabi authorities reportedly hired foreign contractors to hack Qatari government news and social-media sites and post false pro-Iran quotes attributed to the Qatari head of state, Emir Sheikh Tamim Bin Hamad al-Thani. These fabricated comments served as the ostensible reason for a concerted trade and diplomatic boycott of Qatar by some Arab states.[97] The *Washington Post* has reported, though with little detail on offensive cyber aspects, on the role that cyber-skilled intelligence and military veterans from the US have played in UAE strategic activity.[98] The *New York Times* has published in-depth stories on how semi-private companies such as DarkMatter, a UAE company, and NSO, an Israeli company, have helped Gulf authorities, including the UAE, to counter regional rivals in cyberspace.[99]

There are three commercial entities that have been linked in public reporting about UAE offensive operations: DarkMatter, Digital 14 and CPX. Open sources suggest an evolution from each firm to the next as the place where the UAE houses its offensive cyber capability.[100] Judging by public sources, the offensive activity appears to be largely 'project based' with different personnel and partner organisations drawn in as needed rather than creation of a standing governmental organisation dedicated to offensive operations as in other countries.

UAE government ministries are fairly autonomous in acquiring and developing specific cyber capabilities, including offensive ones. Provided there is endorsement at the highest level, there would be few legal restrictions on the country's civil and military authorities to conduct cyber operations compared with countries where cyber policy is subjected to more stringent parliamentary or public scrutiny.

With the aim of countering state-based threats, the UAE Ministry of Defence was reported to have set up its own cyber unit in 2014, but there is no significant public information on any subsequent development.[101] Nevertheless, the armed forces have an incentive to develop cyber capabilities, including for offensive cyber, which could be used to complement conventional military capabilities in conflict zones such as Yemen.[102] The UAE's Special Operations Command has likely used a range of offensive cyber tools on a small scale particularly against armed terrorist groups in Yemen. The development and implementation of these capabilities would be partially outsourced to foreign entities even as the country tries to build its own expertise. From what we know publicly, UAE offensive cyber capabilities are likely to be modest and basic, and they are unlikely to be optimised for military purposes beyond intelligence and targeting functions.

Notes

[1] Shireena Al Nowais, 'Cybersecurity Is Integral Pillar of Digital Transformation, Says UAE Official', *The National*, 4 March 2022, https://www.thenationalnews.com/uae/2022/03/04/cybersecurity-is-integral-pillar-of-digital-transformation-says-uae-official/.

[2] Matthew Hedges, *Reinventing the Sheikhdom: Clan, Power and Patronage in Mohammed bin Zayed's UAE*, (London: Hurst & Co Publishers, 2021), p. 79.

[3] Dubai Electronic Security Center, 'Dubai Cyber Security Strategy', 2017, https://www.desc.gov.ae/cyber-strategy/.

[4] Dubai Electronic Security Center, 'About Us', https://webcache.googleusercontent.com/search?q=cache:hU8DPIVEjM8J:https://www.desc.gov.ae/about-us/&cd=1&hl=en&ct=clnk&gl=sg; and The Supreme Legislation Committee in the Emirate of Dubai, 'Law No. (11) of 2014 Establishing the Dubai Electronic Security Center', 2014, p. 3, https://dlp.dubai.gov.ae/Legislation%20Reference/2014/Law%20No.%20(11)%20of%202014.pdf.

[5] Pat Brans, 'UAE Bolsters Cyber Security', ComputerWeekly.com, 22 April 2022, https://www.computerweekly.com/news/252516180/UAE-bolsters-cyber-security; and UAE Government Portal, 'National Cybersecurity Strategy 2019', 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. Part of the mandate of the UAE Cyber Security Council is to revise the National Cybersecurity Strategy, though the latter's status is currently unknown.

[6] Tori Bergel, 'U.S., UAE and Israeli Cyber Leaders Share the Stage in New York', Jewish Insider, 16 November 2022, https://jewishinsider.com/2022/11/cybertechnyc-amir-rapaport-rob-silvers-israel-united-arab-emirates/.

[7] Department of Justice, 'United States and United Arab Emirates Sign Bilateral Agreement Enhancing Law Enforcement Cooperation', 24 February 2022, https://www.justice.gov/opa/pr/united-states-and-united-arab-emirates-sign-bilateral-agreement-enhancing-law-enforcement; Scott Birch, 'UAE Launches First National Cyber Pulse Innovation Centre', Cyber Magazine, 11 October 2022, https://cybermagazine.com/cyber-security/uae-launches-first-national-cyber-pulse-innovation-centre; and Abu Dhabi Government Media Office, 'Abu Dhabi's Business Delegation to Tel Aviv Deepens the Cross-market Investment Relations & Accelerates Innovation Deployment', 7 September 2022, https://www.mediaoffice.abudhabi/en/economy/abu-dhabis-business-delegation-to-tel-aviv-deepens-the-cross-market-investment-relations-accelerates-innovation-deployment/.

[8] See the website of the International Defence Conference at: https://www.idc-uae.com/.

[9] James Shires and Joyce Hakmeh, 'Is the GCC Cyber Resilient?', Chatham House, March 2020, pp. 14–15, https://www.chathamhouse.org/sites/default/files/CHHJ8019-GCC-Cyber-Briefing-200302-WEB.pdf.

[10] Rori Donaghy, 'Falcon Eye: The Israeli-installed Mass Civil Surveillance System of Abu Dhabi', Middle East Eye, 15 July 2015, https://www.middleeasteye.net/news/falcon-eye-israeli-installed-mass-civil-surveillance-system-abu-dhabi.

[11] Joe Odell, 'Inside the Dark Web of the UAE's Surveillance State', Middle East Eye, 1 March 2018, https://www.middleeasteye.net/opinion/inside-dark-web-uaes-surveillance-state.

[12] Al Bayan, '*Alduktur muhamad hamd alkuayti rayiys al'amn alsaybiranii lihukumat dawlat al'iimarat*' [Dr. Mohammed Hamad Al Kuwaiti, Head of Cyber Security for UAE Government], 5 July 2020, https://www.albayan.ae/across-the-uae/news-and-reports/2020-07-05-1.3903612.

[13] Emirates News Agency, 'Mohammed bin Rashid Approves UAE Environment Policy, UAE Cybersecurity Council and UAE National Media Team', November 29 2020, https://wam.ae/en/details/1395302891155l; and Hussein Nagah, 'UAE Budget Boosts Cybersecurity', Al-Monitor, 20 October 2021, https://www.al-monitor.com/originals/2021/10/uae-budget-boosts-cybersecurity.

[14] See UAE Government Portal, 'Cyber Safety and Digital Security', 18 November 2022, https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security#:~:text=UAE%20Cybersecurity%20Council%20In%20November%202020%2C%20the%20UAE,safe%20and%20strong%20cyber%20infrastructure%20in%20the%20UAE.

[15] Emirates News Agency, 'INEGMA: UAE Leaders Have Worked on Building National Defense 1st Add', 14 December 2014, http://wam.ae/en/details/1395273791751.

[16] President of the United Arab Emirates, 'Federal Decree Law No. 3 of 2012, on the Establishment of the National Electronic Security Authority', 13 August 2012, https://www.lexmena.com/law/en_fed~2012-08-13_00003_2020-06-15/.

17 Intelligence Online, 'Abu Dhabi and Doha Compete in Cyber Offensive Operations', 24 October 2018, https://www.intelligenceonline.com/government-intelligence/2018/10/24/abu-dhabi-and-doha-compete-in-cyber-offensive-operations,108329285-eve; Intelligence Online, 'Verint Poised to Land Major Emirates Interceptions Contract', 18 October 2017, https://www.intelligenceonline.com/international-dealmaking/2017/10/18/verint-poised-to-land-major-emirates-interceptions-contract,108276604-art; and Intelligence Online, 'Abu Dhabi's NSA and Its Helping Hands', April 2017, https://www.intelligenceonline.com/corporate-intelligence/2017/04/05/abu-dhabi-s-nsa-and-its-helping-hands,108228871-art.

18 Intelligence Online, 'NESA, SIA, Darkmatter, BeamTrail Make Up Abu Dhabi's New Interceptions Landscape', 5 June 2019, https://www.intelligenceonline.com/government-intelligence/2019/06/05/nesa-sia-darkmatter-beamtrail-make-up-abu-dhabi-s-new-interceptions-landscape,108359960-eve; and Al-Jazeera, '*al'iimarat tueid haykalat manzumat al'amn alsiybiranii baed fadiha "rifin"*'[UAE Restructuring Cyber-security System After 'Raven' Scandal], 19 August 2019, https://mubasher.aljazeera.net/news/reports/2019/8/19/%D8%A7%D9%84%D8%A5%D9%85%D8%A7%D8%B1%D8%A7%D8%AA-%D8%AA%D8%B9%D9%8A%D8%AF%D9%87%D9%8A%D9%83%D9%84%D8%A9-%D9%85%D9%86%D8%B8%D9%88%D9%85%D8%A9%D8%A7%D9%84%D8%A3%D9%85%D9%86.

19 See the website of the Telecommunications and Digital Government Regulatory Agency at: https://tdra.gov.ae/en/About.

20 UAE Government Portal, 'Overseeing Digital Transformation in the UAE', https://u.ae/en/about-the-uae/digital-uae/digital-transformation/cooperation-and-collaboration/overseeing-digital-transformation-in-the-uae.

21 Hedges, *Reinventing the Sheikhdom: Clan, Power and Patronage in Mohammed bin Zayed's UAE*, p. 79.

22 Access Partnership, 'Access Alert – Introducing the Dubai Digital Authority', 28 June 2021, https://www.accesspartnership.com/access-alert-introducing-the-dubai-digital-authority-dda/.

23 Linda Kay, 'UAE Military to Set Up Cyber Command', Defense World, 30 September 2014, https://www.defenseworld.net/2014/09/30/uae-military-to-set-up-cyber-command.html#.Wnx88q6WbIU.

24 UAE Government Portal, 'Cyber Laws', https://u.ae/en/resources/laws.

25 See, for example, Jenna McLaughlin, 'Deep Pockets, Deep Cover: the UAE Is Paying Ex-CIA Officers to Build a Spy Empire in the Gulf', *Foreign Policy*, 21 December 2017 https://foreignpolicy.com/2017/12/21/deep-pockets-deep-cover-the-uae-is-paying-ex-cia-officers-to-build-a-spy-empire-in-the-gulf/.

26 Intelligence Online, 'Abu Dhabi's NSA and Its Helping Hands', 5 April 2017, https://www.intelligenceonline.com/corporate-intelligence/2017/04/05/abu-dhabi-s-nsa-and-its-helping-hands,108228871-art.

27 DarkMatter has roots in US company CyberPoint, which provided cyber capabilities to the UAE with the approval of US authorities. See Scott Ikeda, 'Prompted by Reuters Investigation, New Legislation Introduced in US to Track and Regulate Foreign Sale of Cyber Capabilities', CPO Magazine, 16 January 2020, https://www.cpomagazine.com/cyber-security/prompted-by-reuters-investigation-new-legislation-introduced-in-u-s-to-track-and-regulate-foreign-sale-of-cyber-capabilities/.

28 Christopher Bing and Joel Schectman, 'Inside the UAE's Secret Hacking Team of American Mercenaries', 30 January 2019, Reuters, https://www.reuters.com/investigates/special-report/usa-spying-raven/.

29 *Times of Israel*, 'UAE-based Intelligence Firm Said Recruiting IDF Veterans From Elite Cyber Unit', 18 October 2019, https://www.timesofisrael.com/uae-based-intelligence-firm-said-recruiting-idf-veterans-from-elite-cyber-unit/.

30 Intelligence Online, 'NESA, SIA, Darkmatter, BeamTrail Make Up Abu Dhabi's New Interceptions Landscape'.

31 Agnes Helou, 'UAE Launches 'Edge' Conglomerate to Address Its 'Antiquated Military Industry', Defense News, 6 November 2019, https://www.defensenews.com/digital-show-dailies/dubai-air-show/2019/11/06/uae-launches-edge-conglomerate-to-address-its-antiquated-military-industry/.

32 Intelligence Online, 'EDGE Takes Up Baton of Mohammed bin Zayed's Defence Ambitions', 27 November 2019, https://www.intelligenceonline.com/government-intelligence/2019/11/27/edge-takes-up-baton-of-mohammed-bin-zayed-s-defence-ambitions,108383675-eve.

33 Intelligence Online, 'UAE Cyber Offensive Champion CPX Hit by Intrusion as Internal Power Battle Rages Around It', 6 June 2022, https://www.intelligenceonline.com/surveillance--interception/2022/06/06/uae-cyber-offensive-champion-cpx-hit-by-intrusion-as-internal-power-battle-rages-around-it,109789748-art; Intelligence Online, 'Emirati

Cyber Offensive Business to Be Switched From Digital14 to CPX', 11 March 2022, https://www.intelligenceonline.com/surveillance--interception/2022/03/11/emirati-cyber-offensive-business-to-be-switched-from-digital14-to-cpx,109739727-art; and Intelligence Online, 'Abu Dhabi Officially Gives Cyber Offence Industry a Makeover', 28 March 2022, https://www.intelligenceonline.com/surveillance--interception/2022/03/28/abu-dhabi-officially-gives-cyber-offence-industry-a-makeover,109763551-art. CPX inherited the cyber-intrusion capabilities of DarkMatter, while other strategic activities of the latter such as vulnerability research were transferred to cyber- and hybrid-warfare developer Digital14, another Emirati company now under the control of EDGE group.

[34] David D. Kirkpatrick, 'Hacking a Prince, an Emir and a Journalist to Impress a Client', *New York Times*, 31 August 2018, https://www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html.

[35] Bing and Schectman, 'Special Report: Inside the UAE's Secret Hacking Team of US Mercenaries'.

[36] Hussein Ibish, 'The UAE's Evolving National Security Strategy', The Arab Gulf States Institute in Washington, 6 April 2017, p. 44, https://agsiw.org/wp-content/uploads/2017/04/UAE-Security_ONLINE.pdf.

[37] Oxford Analytica, 'Gulf States' Offensive Cyber Tools Have Regional Focus', Daily Brief, April 30 2019, https://dailybrief.oxan.com/Analysis/DB243552/Gulf-states-offensive-cyber-tools-have-regional-focus.

[38] Intelligence Online, 'Successor to Mohamed bin Zayed's Cyberattack Outfit DarkMatter Teams With Ex-Mossad Chief's Startup', 1 November 2021, https://www.intelligenceonline.com/surveillance--interception/2021/11/01/successor-to-mohamed-bin-zayed-s-cyberattack-outfit-darkmatter-teams-with-ex-mossad-chief-s-startup,109702102-art; and Intelligence Online, 'Mubadala Strengthens Abu Dhabi Links With Tel Aviv's Cyber Industry', 13 January 2021, https://www.intelligenceonline.com/international-dealmaking/2021/01/13/mubadala-strengthens-abu-dhabi-linkswith-tel-aviv-s-cyber-industry,109633912-art.

[39] The federal e-government programme was established in 2001. Subsequent strategies related to e-government were also published in 2012 and 2013. See Ali M. Al-Khouri, 'eGovernment Strategies The Case of the United Arab Emirates (UAE)', *European Journal of ePractice*, no. 17, 2012, p. 134, https://www.academia.edu/6726926/eGovernment_Strategies_The_Case_of_the_United_Arab_Emirates_UAE_031_.

[40] See UAE Government Portal, 'The UAE Digital Government Strategy 2025', 24 August 2022, 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.

[41] UAE Government Portal, 'Emirates ID', https://u.ae/en/information-and-services/visa-and-emirates-id/emirates-id.

[42] Emirates News Agency, 'President Issues Decree to Adopt UAE's 10 Principles for Next 50 Years', 9 October 2021, https://www.wam.ae/en/details/1395302978675.

[43] Yousef al Otaiba, 'Projects of the 50', https://yousefalotaiba.com/insights/uae-projects-of-the-50/.

[44] Examples include UAE Vision 2021, the 'Fourth Industrial Revolution' strategy and Smart Dubai 2021. See UAE Government Portal, 'The UAE Digital Government Strategy 2025'.

[45] UAE Government Portal, 'Digital Economy Strategy', https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/digital-economy-strategy.

[46] Like Saudi Arabia, smartphone penetration in the UAE was among the highest globally at an estimated 93% in 2021. Mahdi AlBasri et al., 'Digital Health Use and Benefits in KSA and UAE', McKinsey, 16 June 2022, https://www.mckinsey.com/industries/public-and-social-sector/our-insights/growth-opportunities-for-digital-health-in-ksa-and-uae.

[47] Abu Dhabi ranked 28th globally in the Smart City Index 2021, topping the Middle East. Ashwani Kumar, 'Abu Dhabi, Dubai Top Smart City Index 2021 in Middle East', *Khaleej Times*, 29 October 2021, https://www.khaleejtimes.com/uae/abu-dhabi-dubai-top-smart-city-index-2021-in-middle-east.

[48] The UAE ranked 21st globally in the UN E-government Survey 2020. See United Nations Department of Economic and Social Affairs, 'UN E-Government Survey 2020', 10 July 2020, p. 48, https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020.

[49] Telecompaper, 'UAE Has World's Highest FTTH Penetration at 97%', 26 May 2022, https://www.telecompaper.com/news/uae-has-worlds-highest-ftth-penetration-at-97--1425641.

[50] DataReportal, 'Digital 2022: The United Arab Emirates', 9 February 2022, https://datareportal.com/reports/digital-2022-united-arab-emirates.

51 Portulans Institute, ‘Network Readiness Index 2022 – United Arab Emirates’, 2022, https://networkreadinessindex.org/country/united-arab-emirates/.

52 Muzaffar Rizvi, ‘Etisalat Secures Approvals to Raise Foreign Ownership Limit to 49%’, *Khaleej Times*, 7 September 2021, https://www.khaleejtimes.com/telecom/etisalat-secures-approvals-to-raise-foreign-ownership-limit-to-49.

53 Ericsson, ‘Etisalat and Ericsson Partner to Commercially Deploy 5G High-band in the UAE’, 20 June 2021, https://www.ericsson.com/en/news/5/2021/etisalat-and-ericsson-partner-to-commercially-deploy-5g-high-band-in-the-uae-; Agnes Helou, ‘Nokia and Etisalat UAE, From e&, to Launch 5G Private Wireless Networks to Support Enterprise Digital Transformation’, Nokia, 31 March 2022, https://www.nokia.com/about-us/news/releases/2022/03/31/nokia-and-etisalat-uae-from-e-to-launch-5g-private-wireless-networks-to-support-enterprise-digital-transformation/; and Zawya, ‘Etisalat UAE, Part of e&, Collaborates With Huawei Technologies to Launch Telecom Network Slicing Service’, 20 June 2022, https://www.zawya.com/en/press-release/companies-news/etisalat-uae-part-of-e-and-collaborates-with-huawei-technologies-to-launch-telecom-network-slicing-service-ju7dpscz.

54 Karl Flinders, ‘Foreign Professionals and Upskilled Locals in Demand as UAE Sets Ambitious Coding Targets’, ComputerWeekly.com, 22 September 2021, https://www.computerweekly.com/news/252506908/Foreign-professionals-and-upskilled-locals-in-demand-as-UAE-sets-ambitious-coding-targets.

55 Waheed Abbas, ‘UAE Aims to Have the Highest Number of Women Coders: Minister’, *Khaleej Times*, 20 October 2021, https://www.khaleejtimes.com/tech/uae-aims-to-have-the-highest-number-of-women-coders-minister.

56 See United Arab Emirates Minister of State for Artificial Intelligence, ‘UAE National Strategy for Artificial Intelligence 2031’, https://ai.gov.ae/strategy/.

57 UAE Moments, ‘MBZ University of Artificial Intelligence Ranks 30th Globally’, 22 June 2022, https://www.uaemoments.com/mbz-university-of-artificial-intelligence-ranks-30th-globally-486428.html.

58 Thundermark Capital, ‘AI Research Rankings 2022: Sputnik Moment for China?’, Medium, 20 May 2022, https://thundermark.medium.com/ai-research-rankings-2022-sputnik-moment-for-china-64b693386a4.

59 Agnes Helous, ‘Seeking Regional Partners, UAE’s Edge Group Wants to be “Not Just Simply a Vendor”: CEO’, Breaking Defense, 30 June 2022, https://breakingdefense.com/2022/06/seeking-regional-partners-uaes-edge-group-wants-to-be-not-just-simply-a-vendor-ceo/.

60 Intelligence Online, ‘G42 Puts Stamp on UAE’s Geospatial Intelligence Ambitions’, 2 December 2021, https://www.intelligenceonline.com/surveillance--interception/2021/12/02/g42-puts-stamp-on-uae-s-geospatial-intelligence-ambitions,109708581-eve.

61 SpaceWatch.Global, ‘#SpaceWatchGL Coproduction: Yahsat: Paving the Future of Space Industry and Economy’, March 2021, https://spacewatch.global/2021/04/spacewatchgl-coproduction-yahsat-paving-the-future-of-space-industry-and-economy/.

62 Yahsat News, ‘Yahsat And Thuraya to Unveil Advanced Military Satellite Communication Capabilities at Idex 2019’, 14 February 2019, https://www.yahsat.com/en/news-and-media/news/2019/yahsat-and-thuraya-to-unveil-advanced-military-satellite-communication-capabilities-at-idex-2019.

63 Alkesh Sharma, ‘Yahsat Wins $7.7m UAE Government Deal’, *The National*, 29 April 2022, https://www.thenationalnews.com/business/technology/2022/04/29/yahsat-wins-77m-uae-government-deal/.

64 Airbus, ‘Yahsat Signs Contract With Airbus to Build Thuraya’s Next-generation System’, 27 August 2020, https://www.airbus.com/en/newsroom/press-releases/2020-08-yahsat-signs-contract-with-airbus-to-build-thurayas-next-generation; and CBS News, ‘United Arab Emirates Spacecraft Built in Partnership With UC Berkeley Reaches Mars in Historic Mission’, 9 February 2021, https://www.cbsnews.com/sanfrancisco/news/emirates-mars-mission-uae-uc-berkeley-orbits-red-planet/.

65 Defence Procurement International, ‘UAE’s EDGE Group Ranked Among The Top 25 Military Companies in the World’, 15 December 2020, https://www.defenceprocurementinternational.com/news/maritime/edge-has-been-named-among-the-top-25-military-suppliers-in-the-world-by-sipri.

66 Aarti Nagraj, ‘MoIAT, EDB and Edge Sign Agreement to Boost Defence Manufacturing’, *The National*, 21 June 2022, https://www.thenationalnews.com/business/2022/06/21/moiat-edb-and-edge-sign-agreement-to-boost-manufacturing-in-defence/.

67 Helous, ‘Seeking Regional Partners, UAE’s Edge Group Wants to be “Not Just Simply a Vendor”: CEO’; and Haena

Jo , 'Can the UAE Emerge as a Leading Global Defense Supplier?', Defense News, 16 February 2021, https://www.defensenews.com/digital-show-dailies/idex/2021/02/15/can-the-uae-emerge-as-a-leading-global-defense-supplier/.

68 James Thorpe, 'New Report Reveals UAE's Cyber Threat Landscape', International Security Journal, 12 August 2021, https://internationalsecurityjournal.com/uaes-threat-landscape/.

69 Bindu Rai, 'There are 50,000 Cyber-attacks Daily in the UAE; Here's How You Can Help', Zawya, 12 May 2023, https://www.zawya.com/en/business/technology-and-telecom/there-are-50-000-cyber-attacks-daily-in-the-uae-heres-how-you-can-help-sxbtbmgv.

70 Ella Hutchison, 'UAE Records 14% Drop in Cyberattacks in 2022, SonicWall Cyber Threat Report Reveals', Intelligent CISO, 22 March 2023, https://www.intelligentciso.com/2023/03/22/uae-records-14-drop-in-cyberattacks-in-2022-sonicwall-cyber-threat-report-reveals/.

71 Clyde & Co, 'UAE Updates Cybercrime Law', 30 March 2022, https://www.clydeco.com/en/insights/2022/03/uae-updates-cybercrime-law.

72 Telecommunications Regulatory Authority, 'UAE Information Assurance Regulation, Version 1.1', March 2020, https://u.ae/-/media/guidelines/Guidelines-2020/UAE-IA-Regulation-v11-1-English-only.ashx.

73 UAE Government Portal, 'Cyber Safety and Digital Security', 18 November 2022, https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security; ITP.net, 'UAE Cyber-security Authority Unveils Policies, Standards', 25 June 2014, https://www.itp.net/security/598777-uae-cyber-security-authority-unveils-policies-standards; and National Electronic Security Authority, 'Critical Information Infrastructure Protection (CIIP) Policy', https://webcache.googleusercontent.com/search?q=cache:R2aju-huUfUJ:https://lms.saiuae.gov.ae/pluginfile.php/3263/mod_glossary/attachment/5/Critical%2520Information%2520Infrastructure%2520Protection%2520%2528CIIP%2529%2520Policy.pdf+&cd=13&hl=en&ct=clnk&gl=uk.

74 Sarah Foster, 'Sheikh Mohammed bin Rashid Announces Five-year Budget for UAE', *The National*, 12 October 2021, https://www.thenationalnews.com/uae/government/2021/10/12/sheikh-mohammed-bin-rashid-announces-five-year-budget-for-uae/.

75 Emirates News Agency, 'UAE Cybersecurity Council Holds Third Meeting in 2021', 30 March 2021, https://wam.ae/en/details/1395302922850; and Emirates News Agency, 'UAE Cybersecurity Council Holds First Meeting Remotely', 28 January 2021, https://www.wam.ae/en/details/1395302905120.

76 Datatechvibe, 'UAE Cyber Security Council Partners With CPX Holdings', 14 October 2022, https://datatechvibe.com/news/uae-cyber-security-council-cpx-partner-to-deliver-solutions-for-threat-assessment-and-response/.

77 Telecommunications and Digital Government Regulatory Authority, 'Monitoring and Response', https://tdra.gov.ae/en/aecert/services/monitoring-and-response.

78 National Electronic Security Authority, 'Protection of Critical Information Infrastructure (CIIP) Policy', 2023, https://u.ae/-/media/Documents-2023/Critical-Information-Infrastructure-Protection-CIIP-Policy.ashx.

79 Dan Rayward, 'UAE, Israel Ink Pivotal Joint Cyber-Threat Intelligence Agreement, Dark Reading, 29 June 2023, https://www.darkreading.com/threat-intelligence/uae-israel-joint-cyber-threat-intelligence-agreement.

80 UAE Government Portal, 'Cyber Safety and Digital Security', https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security.

81 Hamdi Saad, '*muhamad alkuayti: tansiq hukumiun kamil liltaeamul astbaqyaan mae altahdidat*' [Mohammed al-Kuwaiti: Full Government Coordination to Deal Proactively with Threats], *Al Khaleej*, 21 March 2022, https://bit.ly/3GM1JVS.

82 See the website of Dubai Financial Services Authority at: https://www.dfsa.ae/what-we-do.

83 Gulf News, 'Central Bank of the UAE Establishes Cyber Security Operations Centre', 2 November 2021, https://gulfnews.com/business/banking/central-bank-of-the-uae-establishes-cyber-security-operations-centre-1.83392020.

84 Federal Authority for Nuclear Regulation, 'Cyber Security Regulatory Program at the United Arab Emirates Nuclear Power Plant', 2020, https://conferences.iaea.org/event/181/contributions/15574/attachments/8761/11750/ID_239_Muhairi_Poster.pdf.

85 Consultancy-me.com, 'UAE's Cyber Security Council Selects External Partners', 6 June 2022, https://www.consultancy-me.com/news/5051/uaes-cyber-security-council-selects-external-partners.

86 Manda Banda, Palo Alto Networks Offers Automated Protection for UAE-based G42', Intelligent CIO, 28 February 2022, https://www.intelligentcio.com/me/2022/02/28/palo-alto-networks-offers-automated-protection-for-uae-based-g42/#.

87 Emirates News Agency, 'National Cyber Security Council, CPX Sign MoU to Improve Cyber Maturity of Government Entities', 20 March 2022, https://wam.ae/en/details/1395303031684; and Gulf Business, 'Intersec 2022: Injazat Signs MoU With UAE National Cyber Security Council', 17 January 2022, https://gulfbusiness.com/intersec-2022-injazat-signs-mou-with-uae-national-cyber-security-council/.

88 Brans, 'UAE Bolsters Cyber Security', ComputerWeekly.com.

89 Gulf News, 'Dubai Initiative Gets Started on Cyber Workforce With "Cyber Node"', 14 April 2022, https://gulfnews.com/business/dubai-initiative-gets-started-on-cyber-workforce-with-cyber-node-1.87185561.

90 *Khaleej Times*, 'UAE Cybersecurity Council Launches "National Bug Bounty Programme"', 1 August 2021, https://www.khaleejtimes.com/local-business/uae-cybersecurity-council-launches-national-bug-bounty-programme.

91 International Telecommunication Union, 'Global Cybersecurity Index 2020', 2021, p. 25, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

92 Woodrow Bellamy, 'UAE Signs New ICAO Aviation Cybersecurity Collaboration Agreement', Aviation Today, 6 April 2022, https://www.aviationtoday.com/2022/04/06/uae-signs-new-icao-aviation-cybersecurity-collaboration-agreement/.

93 See the website of the International Exhibition for National Security and Resilience at: https://www.isnrabudhabi.com/.

94 James Shires and Joyce Hakmeh, 'Is the GCC Cyber Resilient', Policy Commons, 9 March 2020, https://policycommons.net/artifacts/1423474/is-the-gcc-cyber-resilient/2037742/.

95 United Nations General Assembly, 'Countering the Use of Information and Communications Technologies for Criminal Purposes: Report of the Third Committee', 25 November 2019, https://digitallibrary.un.org/record/3837326.

96 Sarah Foster, 'Sheikh Mohammed bin Rashid Announces Five-year Budget for UAE', *The National*, 12 October 2021, https://www.thenationalnews.com/uae/government/2021/10/12/sheikh-mohammed-bin-rashid-announces-five-year-budget-for-uae/.

97 Zach Dorfman and Breanne Deppisch, 'The Rise of the Rest: Maturing Cyber Threats Beyond the Big Four', The Aspen Institute, November 2019, https://www.aspeninstitute.org/programs/threat-assessment-2019/; and Karen DeYoung and Ellen Nakashima, 'UAE Orchestrated Hacking of Qatari Government Sites, Sparking Regional Upheaval, According to US Intelligence Officials', *Washington Post*, 16 July 2017, https://www.washingtonpost.com/world/national-security/uae-hacked-qatari-government-sites-sparking-regional-upheaval-according-to-us-intelligence-officials/2017/07/16/00c46e54-698f-11e7-8eb5-cbccc2e7bfbf_story.html.

98 Craig Whitlock and Nate Jones, 'UAE Relied on Expertise of Retired U.S. Troops to Beef Up Its Military, *Washington Post*, 18 October 2022, https://www.washingtonpost.com/investigations/interactive/2022/uae-military-us-veterans/.

99 Mark Mazzetti et al, 'A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments', *New York Times*, 21 March 2019, https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html.

100 Cyber Warfare Asia, 'Abu Dhabi Cyber Offensive Arm Digital 14 Gets a New Face: CPX', 7 April 2022, https://mahdiabbastech.medium.com/abu-dhabi-cyber-offensive-arm-digital-14-gets-a-new-face-cpx-3eea37598d57.

101 Bindiya Thomas, 'UAE Military to Set Up Cyber Command', DefenseWorld.net, 30 September 2014, https://www.defenseworld.net/2014/09/30/uae-military-to-set-up-cyber-command.html. On at least one occasion, DarkMatter has denied any role in offensive cyber operations.

102 Oxford Analytics, 'Gulf States' Offensive Cyber Tools Have Regional Focus', 30 April 2019, https://www.emerald.com/insight/content/doi/10.1108/OXAN-DB243552/full/html.