The Role of Foreign Expertise in the UAE's Strategy for Cyber Security

By Al Stovall, Contributing Editor

The United Arab Emirates (UAE) is in the midst of a campaign to establish itself as a regional cyber power with sophisticated indigenous capabilities rivaling those of Iran and Israel. With this understanding, the campaign consists of three distinct elements: the completion of legal, policy, and administrative reform to organize cyber-related government bodies and bring the UAE in-line with international cybersecurity standards; the use of foreign and for-hire cyber specialists to surpass the limits of current operational capabilities while growing indigenous cyber expertise; and the exploitation of indigenous cyber expertise to successfully and independently complete cyber operations and achieve cybersecurity goals. This piece will touch on key portions of the first element but focus on the publicly known aspects of the second.

Key Cyber-Related Reform

The UAE has enacted a number of reforms to best organize its government and its national-level approach to cyber affairs. Of those reforms, the most transformative concerning national cyber security are:

- Federal Decree No. 3 of 2003 that established the Telecommunications Regulatory Authority (TRA) to regulate the Information and Communication Technologies (ICT) sector.[1]
- Resolution 5/89 of 2008 that established the UAE Computer Emergency Response Team (aeCERT) as a subsidiary of the TRA and tasked it with improving standards and protects ICT infrastructure.[2]
- Federal Decree No. 3 of 2012 that established the National Electronic Security Authority (NESA), now known as the Signals Intelligence Agency (SIA), under the Supreme Council for National Security to oversee national efforts to improve the cybersecurity of the ICT sector and protect it from cyber attacks.[3]

جهـــاز اســـتخبارات الإشـــارة
SIGNALS INTELLIGENCE AGENCY
UNITED ARAB EMIRATES الإمارات العربية المتحدة

- The SIA's UAE information Assurance Standards (UAE IAS), Critical Information Infrastructure Policy (CIIP), and National Cyber Security Strategy (NCSS) that outline a specialized national framework for UAE cybersecurity issues while still including key provisions of ISO/IEC 27001 and NIST.[4]
- The formation of a cyber command to operate alongside the NESA in formulating cybersecurity strategies and protecting key ICT infrastructure similar in mission and scope to the US Army's Cyber Protection Brigade.[5]

The Cyber Campaign's Second Element

The UAE has a known history of utilizing foreign and for-hire cyber specialists. It has used their expertise as an imported force multiplier, a source for training, and even a complete replacement for Emirati specialists.

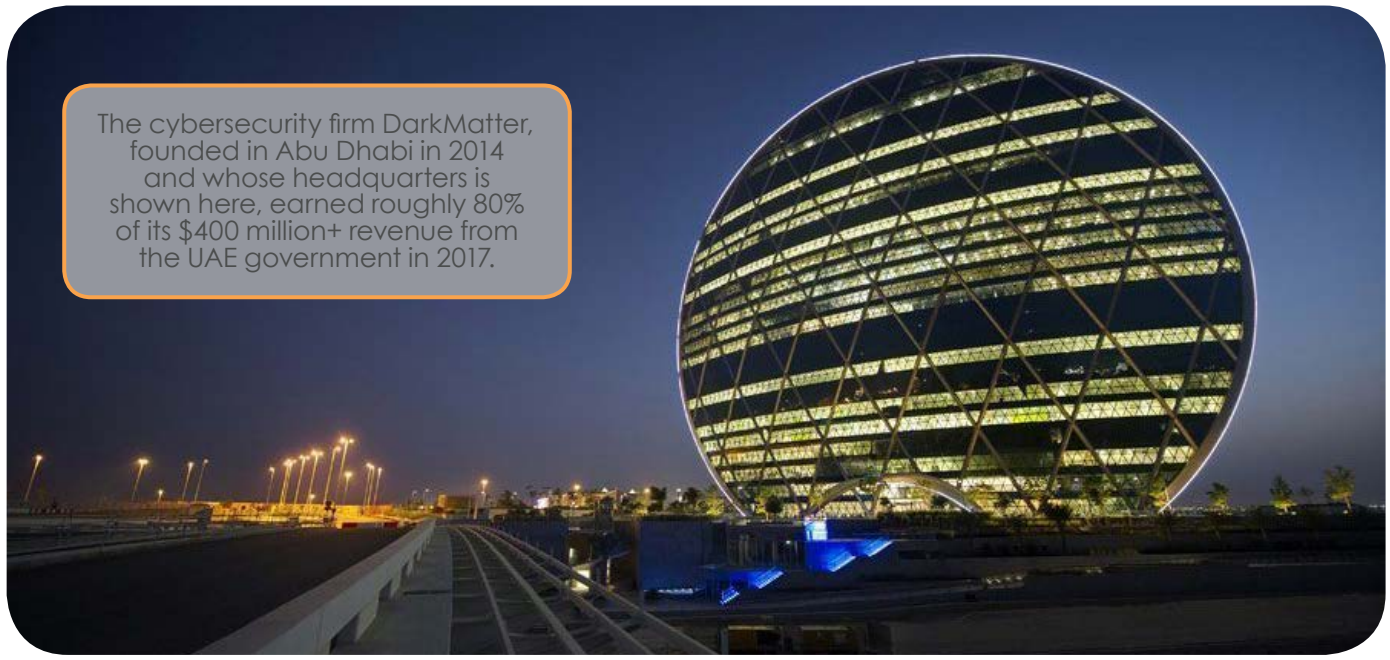
Foreign Expertise as a Tool of Instruction

The UAE has often used foreign expertise to help train and foster growth in Emirati cyber specialists. It has solicited help from governments, private companies, universities, and individuals all to the same end. Some of this training focuses on future generations of specialists, such as Cyber Quest, which the Edinburgh International Science Festival designed at the request of the NESA, or the four-day cyber workshop for students at Khalifa University that Raytheon organized.[6] The UAE also maintains connections to select institutions around the world, whose students can receive scholarships for their work in cybersecurity and other critical fields of study and attend select US and UAE universities.[7] However, the UAE's use of foreign expertise for professional development has also been successful. For example, when the UAE was formulating the NESA, specialists from the US Intelligence Community were "involved in everything from helping select a safe site with access to power and fiber connectivity to determining which buildings would be public and which classified."[8]

Foreign Expertise as an Enabler

The cybersecurity firm DarkMatter, founded in Abu Dhabi in 2014, earned roughly 80% of its $400 million+ revenue from the UAE government in 2017. The firm has experienced explosive growth in personnel and profits, tripling in size since its founding and doubling its revenue from 2016. It has also come to advise key regulatory and oversight bodies related to the UAE ICT sector including the SIA, with which it shared a building for its headquarters.[9] The firm's expansion is a product of its aggressive and successful pursuit of employees from major international tech companies such as Google, Qualcomm, Samsung, Intel Corporation, and BlackBerry, foreign intelligence agency analysts including those from the CIA and NSA, and solo internet-based hackers.[10] Since its founding, activists have raised concerns that DarkMatter was using its expertise to improve the UAE's capability to conduct unethical targeted surveillance, particularly against human rights campaigners.[11] There have also been allegations that DarkMatter has used its growing capabilities to enable more advanced offensive cyber operations. These rumors became even more credible after DarkMatter acquired a number of employees from Maryland-based CyberPoint International, which was revealed to have been selling surveillance equipment to repressive regimes with the Italian cyber firm Hacking Team.[12]

Regardless of the amount of truth to the allegations of DarkMatter's unsavory behavior, it has provided critical support to the UAE's cyber operations and has positioned itself to continue to do so for the foreseeable future. Moreover, the massive amount of personnel imported from abroad indicates that the UAE has an appetite for foreign specialists able to provide advanced cyber skillsets.



Foreign Expertise As a Substitute

The UAE's use of foreign and for-hire specialists to support cyber operations as replacements for Emiratis is more sparsely documented in public. However, it has become somewhat more well-known after the failed recruitment of Simone Margaritelli. The founder of DarkMatter, Faisal al-Bannai, reportedly reached out to Margaritelli through an intermediary at the US-Israeli cyber firm Verint Systems and flew him to the UAE to recruit him into a brain trust of international cybersecurity professionals well-versed in large-scale surveillance software.[13] The group was to custom create software for the UAE government "capable of intercepting, modifying, and diverting (as well as occasionally obscuring) traffic on IP, 2G, 3G, and 4G networks."[14] Apparently, the UAE government launched the Falcon Eye surveillance system during his visit and the spread of hardware probes deployed with the system already would already provide the government with a platform for mass data interception and manipulation.[15] The UAE had reportedly developed its own software but that failed to scale appropriately, which inspired them to turn to a team of foreign specialists.[16] The group's leadership offered Margaritelli a $20,000 per month tax-free salary because they were so intent on his participation.[17]

The Cyber Campaign in Context

The aggressive recruitment tactics of DarkMatter and the Emirati government's rush to improve UAE cybersecurity capabilities begin to make sense when taken in proper context. Between 2011 and 2016 the UAE experienced a 500% increase in cyber attacks, receiving 5% of all attacks globally by mid-2016, which placed it behind only the United States as the most popular state target.[18] During 2015, two million residents and one-third of the state's private firms reported being the victims of security breaches.[19] Nine months into 2016 the situation had failed to improve with reports of most firms being entirely "incapable of protecting themselves" and completely devoid of staff cybersecurity training.[20] In 2017 over half of the UAE online adult population were victims of cybercrime, contributing to a total of 3.72 million victims and over $1 billion worth in losses.[21] As a state with less than 10 million citizens and limited indigenous cyber expertise that has to address cybercrime on this level, it seems a natural solution to import specialists as fast and in as great a number as possible.[22] The UAE has demonstrated its ability to plan and execute important reforms and import and mobilize talent from abroad, but it won't find success until an informed citizenry is the backbone of its cybersecurity.

Al Stovall is a Fellow at the Military Cyber Professionals Association and a graduate of the Walsh School of Foreign Service at Georgetown University. He has supported publications as a writer, researcher, and editor in both the public and private sectors focusing on evolving security dynamics in the Arab state system and Southwest Asia. He is interested in developing cyber expertise and contributing to the next generation of cyber savvy leaders in the defense industry and Intelligence Community.

1."Federal Law by Decree No. 3 of 2003 Regarding the Organization of Telecommunications Sector, as amended," Telecommunication Regulatory Authority, last modified October 2008, p. 12; "About TRA| Vision, Mission & Values," Telecommunications Regulatory Authority, last modified 2018, tra.gov.ae/en/about-tra/about-tra-vision-mission-and-values.aspx.
2."The UAE Cabinet" last modified 2018, www.government.ae/en/about-the-uae/the-uae-government/the-uae-cabinet;
"Our Story and Goals," aeCERT, tra.gov.ae/aecert/en/about-us/our-story-and-goals.aspx.
3.Shiekh Sadab, "A Brief Insight to NESA Compliance," Paladion, last modified January 12, 2016, https://www.paladion.net/blogs/insight-to-uae-nesa-compliance; Benjamin Hopps & Stuart Patterson, "Cybersecurity: United Arab Emirates," Getting the Deal Through, last modified January 2018, https://gettingthedealthrough.com/area/72/jurisdiction/33/cybersecurity-united-arab-emirates.
4.Ibid.
5.Bindiya Thomas, "UAE Military to Set Up Cyber Command," Defense World, last modified September 30, 2014, http://www.defenseworld.net/news/11185/UAE_Military_To_Set_Up_Cyber_Command.
6.Roberta Pennington, "Nurturing the cyber security specialists of the future," The National, last modified April 9 2017, https://www.thenational.ae/business/technology/nurturing-the-cyber-security-specialists-of-the-future-1.60828; "Training Cyber Defenders Around the World," Raytheon, last modified January 11, 2018, https://www.raytheon.com/news/feature/training-cyber-defenders-around-world.
7."Tamayuz Scholarship Program," Khalifa University,last modified 2015, kustar.ac.ae/source/admissions/ug-scholarship2015.pdf.
8.Jenna McLaughlin, "Deep Pockets, Deep Cover: The UAE Is Paying Ex-CIA Officers to Build a Spy Empire in the Gulf," Foreign Policy, last modified December 21, 2017, http://foreignpolicy.com/2017/12/21/deep-pockets-deep-cover-the-uae-is-paying-ex-cia-officers-to-build-a-spy-empire-in-the-gulf.
9.Alexander Cornwell, "Emerging Gulf State cyber security powerhouse growing rapidly in size, revenue," Reuters, last modified February 1, 2018, https://www.reuters.com/article/us-emirates-cyber-darkmatter/emerging-gulf-state-cyber-security-powerhouse-growing-rapidly-in-size-revenue-idUSKBN1FL451;
John Everington, "DarkMatter recruits technology veteran Karim Sabbagh as new CEO," The National, last updated March 5, 2018, https://www.thenational.ae/business/technology/darkmatter-recruits-technology-veteran-karim-sabbagh-as-new-ceo-1.710309; Jenna McLaughlin, "Spies for Hire: How the UAE is Recruiting Hackers to Create the Perfect Surveillance State," The Intercept, last modified October 24, 2016, https://theintercept.com/2016/10/24/darkmatter-united-arab-emirates-spies-for-hire.
10.Nour Al Ali & Mathew Martin, "UAE-Based Cyber Security Firm DarkMatter Doubles Revenue in 2017 to $400M," Insurance Journal, last modified March 1, 2018, https://www.insurancejournal.com/news/international/2018/03/01/482013.htm; McLaughlin, "Spies."
11.Jon Gambrell, "U.A.E. Cyber Firm DarkMatter Slowly Steps Out of the Shadows," Bloomberg, last modified February 1, 2018, https://www.bloomberg.com/news/articles/2018-02-01/uae-cyber-firm-darkmatter-slowly-steps-out-of-the-shadows.
12.Andy Greenberg, "Hacking Team Breach Shows a Global Spying Firm Run Amok," Wired, last modified July 6, 2015, https://www.wired.com/2015/07/hacking-team-breach-shows-global-spying-firm-run-amok; McLaughlin, "Spies."
13.Ron Donaghy, "EXCLUSIVE: UAE recruiting 'elite task force' for secret surveillance state," Middle East Eye, last modified August 1, 2016, http://www.middleeasteye.net/news/exclusive-uae-elite-task-force-security-secret-surveillance-state-135285760.
14.Simone Margaritelli, "How the United Arab Emirates Intelligence Tried to Hire Me to Spy on Its People" last modified July 27, 2016, evilsocket.net/2016/07/27/How-The-United-Arab-Emirates-Intelligence-Tried-to-Hire-me-to-Spy-on-its-People.
15.Donaghy, "EXCLUSIVE."; "Abu Dhabi launches 'Falcon Eye,'" Gulf News, last modified July 13, 2016, http://gulfnews.com/news/uae/government/abu-dhabi-launches-falcon-eye-1.1861841.
16.McLaughlin, "Spies."
17.Donaghy, "EXCLUSIVE."
18.Nada Altaher, "UAE a target of 5 per cent of global cyber attacks," Gulf News, last modified May 12, 2016, https://gulfnews.com/news/uae/crime/uae-a-target-of-5-per-cent-of-global-cyber-attacks-1.1826610; Naushad K. Cherrayil, "UAE is ranked second most targeted country after US," Zawya, last modified August 22, 2016, https://www.zawya.com/mena/en/story/UAE_is_ranked_second_most_targeted_country_after_the_US-GN_22082016_230837.
19."A third of UAE firms hit by cyber security breaches," Gulf News, last modified December 20, 2015, https://gulfnews.com/business/sectors/technology/a-third-of-uae-firms-hit-by-cyber-security-breaches-1.1640766.
20.Jennifer Bell, "UAE companies 'wide open' to cyber attacks due to lack of staff training," The National, last modified September 13, 2016, https://www.thenational.ae/business/technology/uae-companies-wide-open-to-cyber-attacks-due-to-lack-of-staff-training-1.220114; Hussein Ibish, "The UAE's Evolving National Security Strategy," The Arab Gulf States Institute in Washington, last modified April 6, 2017, p. 43.
21.Bernd Debusmann Jr., "Over 3m UAE consumers lost $1bn to cybercrime in 2017," Arabian Business, last modified January 23, 2018, http://www.arabianbusiness.com/technology/388166-over-3m-uae-consumers-lost-1bn-to-cybercrime-in-2017.
22."United Arab Emirates Population" last modified 2018, http://www.worldometers.info/world-population/united-arab-emirates-population.

Image credits (in order of appearance): Watan Properties Development, InfoSecurity Middle East, Arabian Business