Virtual War: The Qatar-UAE Battle of Narratives

Lucas Winter

FOREIGN MILITARY STUDIES OFFICE

Open Source, Foreign Perspective, Underconsidered/Understudied Topics

The Foreign Military Studies Office (FMSO) at Fort Leavenworth, Kansas, is an open source research organization of the U.S. Army. It was founded in 1986 as an innovative program that brought together military specialists and civilian academics to focus on military and security topics derived from unclassified, foreign media. Today FMSO maintains this research tradition of special insight and highly collaborative work by conducting unclassified research on foreign perspectives of defense and security issues that are understudied or unconsidered.

Author Background

Lucas Winter is an analyst on the Middle East for the Foreign Military Studies Office (FMSO) at Fort Leavenworth, KS. He has an M.A. in International Relations from Johns Hopkins SAIS and was an Arabic Language Flagship Fellow in Damascus, Syria in 2006-2007. He has extensive practical and academic experience in the Middle East and North Africa and is proficient in Arabic. His research focuses on understudied security issues and foreign perspectives on the operational environment in Arabic-speaking countries, particularly Egypt, Yemen, Gulf countries and the Levant. His work has been published in various security, policy and military education journals, including Current History, Middle East Policy, Middle East Quarterly, CTC Sentinel, Infantry Magazine, Engineer: The Professional Bulletin of Army Engineers and The Infantry Bugler.

Virtual War: The Qatar-UAE Battle of Narratives

Lucas Winter

Over the past decade, strategic competition between Qatar and the UAE has evolved into low-level information warfare. What began as disagreements on foreign policy in the wake of the Arab Spring has escalated into a conflict to shape and control information flows in cyberspace. Although not always visible, Qatari-Emirati competition has become a persistent feature of the regional Operational Environment (OE). Their competition in the cyber-information sphere is part of a broader competition for influence involving Turkey, Qatar and their allies, on the one hand, and Saudi Arabia, Egypt, the UAE and their allies, on the other.[1] One of Qatar's main contributions to the Turkish-led axis is the employment of Arabic-language media outlets to influence local and foreign perceptions of the OE. The adversarial Qatar-UAE relationship has more recently morphed into a nascent cyberconflict to control not only the narrative but also digital data and information. Hoping to become hubs of the new digital economy, both countries are investing in cybersecurity and artificial intelligence (AI) technologies in ways that will enhance their capabilities to shaper perceptions of the OE.[2] Their conflict will continue to be a dynamic factor shaping the regional OE, and its evolution highlights the changing character of information war.

\

[1] Since the 2016 coup attempt against the Erdogan government, Turkey has been openly competing with Egypt and the UAE for influence in Libya, the Eastern Mediterranean, the Red Sea/Horn of Africa and the North African Sahel.

[2] "The primacy of information" to future battlefields is underlined by TRADOC pamphlet 525-92, "The Operational Environment and the Changing Character of Warfare," which sees information as becoming "the most important and most useful tool at all levels of warfare." See: "The Operational Environment and the Changing Character of warfare," TRADOC Pamphlet 52592. https://adminpubs.tradoc.army.mil/pamphlets/TP525-92.pdf (Accessed 2/20/2020). See also: Singer, P. W. & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. Eamon Dolan Books.

COMPETING NARRATIVES IN THE WAKE OF THE ARAB SPRING

The popular revolts of late 2010 and early 2011 created divisions at all levels of Arab society: families were split between the pro- and anti-government poles, communities were destroyed by internal fighting and government attacks, and longstanding regimes collapsed in a matter of weeks. Otherwise cordial interstate relations became fraught, as governments across the region were forced to take a position on events outside their borders, if nothing else to prevent protests from cascading into their own countries. Qatar emerged as the protest movement's key ally, as coverage by its flagship news channel *al-Jazeera* imbued scattered and often spontaneous protests with a sense of unity, grandeur and purpose.[3] Communicating through social media, smartphone users offered the network a trove of first-hand accounts, many of which were then curated and disseminated to its substantial global audience. Beginning in late 2010, *al-Jazeera* played an outsized role in the political fortunes of Tunisia, Egypt, Libya, Yemen, Syria and, to a lesser degree, Bahrain. Generally speaking, its narrative portrayed protests in these countries as brave and noble revolts against tyrannical regimes. Its international roster of eyewitnesses, reporters, analysts and pundits argued for replacing longstanding regimes with electoral democracies, while dismissing status quo defenders as regime apologists. The narrative resonated across the globe.

Most other governments in the region were less sanguine about the region-wide protest movement. While all governments objected to *al-Jazeera*'s coverage in their own countries, fellow Gulf Cooperation Council (GCC) members Saudi Arabia and the UAE objected strongly to its coverage of protests in fellow GCC member Bahrain. Under the aegis of the joint GCC military forces ("the Peninsula Shield"), Saudi Arabia and the UAE deployed security forces to quell the Bahraini protest movement in the spring of 2011, and *al-Jazeera*'s coverage of that country faded away in the following months. *Al-Jazeera*'s

[3] In the decade prior, the Qatari government had amassed "soft power" in part thanks to al-Jazeera, which established itself as the mouthpiece of the "Arab Street." The Qatari government also gained influence abroad through financial assistance and third-party mediation efforts.

critics in Saudi Arabia and the UAE accused it of being an instrument of Qatari meddling in the affairs of others.

By 2012, the Arab Spring's mass protest movements had either devolved into armed rebellions (Syria and Libya) or birthed negotiated political settlements (Tunisia, Egypt, Yemen). Muslim Brotherhood-affiliated movements and parties emerged as the best organized political forces, bolstered by extensive and approving airtime on *al-Jazeera*. By early 2013, previously banned Muslim Brotherhood-affiliated parties were either in control of the government or considered the main opposition party in Egypt (Freedom and Justice Party), Tunisia (al-Nahda) and Yemen (Islah). Muslim Brotherhood-affiliated political groups and militias were also dominant in the Syrian and Libyan oppositions.

Qatari control over the post-Arab Spring narrative was curtailed in the summer of 2013, when the government of Mohammed Morsi in Egypt was toppled by a well-organized popular movement backed by Egypt's military, political and media elite. The overthrow was supported publicly by the UAE and Saudi Arabia, who replaced Qatar as the Egyptian government's main political and financial backer. Egypt's new military-led government, headed by Abdel Fattah Sisi, took control of the national media and joined its Saudi and Emirati counterparts in accusing Qatar of meddling in the affairs of others and empowering religious fanatics. *Al-Jazeera* and like-minded media outlets, in turn, took a highly critical tone of the new Egyptian government, portraying it as a corrupt, violent military dictatorship, beholden to its Saudi and Emirati benefactors, and bent on nefariously subduing its populace. [4]

[4] See for example: "Egypt's dirty war (part I): Baptised in blood," *al-Araby al-Jadid, 1 February 2019.* https://www.alaraby.co.uk/english/comment/2019/2/1/egypts-dirty-war-part-ii-surveillance-for-all (Accessed 2/20/2020).

By early 2014, Egypt had joined the UAE, Saudi Arabia and Bahrain, in an alliance to oppose Qatari foreign policy. "The Quartet," as it came to be called, accused Qatar of sponsoring terrorist entities across the region. In early 2014, Quartet countries withdrew their ambassadors from Doha to protest alleged continued Qatari meddling in the affairs of others, its promotion of "religious extremism," and its support for the Muslim Brotherhood.[5] Quartet countries also began backing Qatari opponents in Libya and Yemen. Saudi and Emirati media decried Qatar's relations with Turkey and Iran, as well as with Hamas, the Houthis and Hezbollah. The Qatari government, meanwhile, deepened its ties with Turkey, whose government also backed Muslim Brotherhood movements during the Arab Spring and more broadly supported the "moderate Islam" model promoted in Qatari media. The failed 2016 coup attempt in Turkey, which was supported by government-controlled media in Egypt and the UAE, further hardened the distinction between the two emerging strategic blocs.

Prior to 2011, the Middle East strategic map was largely viewed through the prism of Saudi-Iranian competition and the reinforcing Sunni-Shi'ite sectarian divisions, which were considered the region's primary fault line. By 2014, however, the fissure between Qatar and the Quartet pointed to a new strategic reconfiguration, with three rather than two competing poles of regional power: the Saudi-Emirati-Egyptian-Bahraini "Quartet" and allied Arab monarchies; the Iranian-backed "Resistance Axis," including the Syrian government, Yemen's Houthi Movement, Hezbollah, and Iranian-backed Iraqi parties and movements; and a "Moderate Islam" alliance centered on Turkey and Qatar and also including Islamist political parties and militias throughout the region, most of them affiliated with the Muslim Brotherhood.

[5] The ambassadors returned 10 months later purportedly after Qatar agreed to change its ways, though Quartet countries would in 2017 claim that Qatar had not held up its end of the bargain.

In the post-Arab Spring era, leaders and citizens of Qatar and the UAE consider their countries as beacons of a brighter regional future. Before 2011, the dynamics of their bilateral relations were marginal to regional politics; since then, competition between them has evolved into a key driver of regional political dynamics.

CYBERSPACE AND NARRATIVES

On 24 May 2017, shortly after midnight local time, the state-run Qatar News Agency (QNA) posted controversial statements to its social media accounts. Attributed to the young, recently appointed Emir of Qatar, Sheikh Tamim Bin Hamad al-Thani, the statements expressed Qatari goodwill toward Israel, Iran, Hamas and Hezbollah. They quickly trended on social media and were reported on as fact by Emirati (and Saudi) news stations. A few hours passed before Qatari officials announced that the statements had been fabricated by hackers who, for three long hours, had gained control over the QNA network, including access to websites and social media accounts. Saudi and UAE media ignored Qatar's allegations, continued treating the statements as fact while dismissing Qatari claims of a hack as dubious if not irrelevant, arguing that even if the statements had not been made they reflected Qatar's foreign policy orientation. Qatar would ultimately blame the QNA hack on the UAE.[6]

The following week, unnamed hackers released a cache of emails belonging to the UAE's ambassador to the United States. The correspondence pointed to an influence campaign, orchestrated by the UAE, aimed at tarnishing Qatar's image among Washington's political elite. The leaks came from a "hacktivist group" calling itself "GlobalLeaks," of whom no verifiable public details have emerged. A few days later, on 5 June, the Quartet officially declared a full embargo on Qatar, including closing off its only land border with Saudi Arabia. The Qatari government was given an expansive list of demands for lifting the

[6] It officially blamed a "Saudi piracy cell" working for an Azerbaijan-based company from the UAE, in coordination with Turkish companies. Qatari officials, though, emphasized that the attack had been launched from UAE territory and ultimate blame lay there.

embargo, including shutting down *al-Jazeera*. That month, *al-Jazeera* reported that it had warded off several attempted cyberattacks, while the UAE and Saudi Arabia also reported an uptick in cybersecurity incidents.

The events of 2017 shifted the nature of Qatari-Emirati competition, from being primarily the purview of government officials, spokespeople, journalists, analysts and authors, to one where coders, influencers, trolls and cybersecurity experts played a vital role. The war of narratives, which had until then largely played out in traditional media channels, now morphed into an information war in which the integrity of the data, not just the information itself, was being contested. While cyberspace technicians have become indispensable in influence campaigns across the globe, the fact that Qatar and the UAE are among the most "wired" and social media-savvy societies in the world make coding expertise more relevant than in most places.[7] Futurism, one might say, is part of their modern national identities.[8]

Indeed, the expectation that technology will solve looming economic and climactic challenges is a virtual article of faith in both countries' strategic planning documents.[9] Their main urban centers – Doha in Qatar, Dubai and Abu Dhabi in the UAE – all aim to be retrofitted as "smart cities" in the near future. Protecting the integrity of the virtual reams of data produced by Internet of things (IoT) technologies, which are likely to see rapid adoption in these countries, further boosts the cybersecurity and digital

[7] For instance in Symantec's February 2019 Internet Security Threat Report (https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf), Qatar and the UAE rank in the top twenty globally in terms of "malicious email rate by country." Fellow GCC member Saudi Arabia ranks first globally.

[8] At the same time, this futuristic orientation coexists with "clinging desperately to the moral rules of the past" to create a hybrid between the future and the past that some refer to as "Gulf Futurism." See: "The desert of the unreal," *Dazed Digital*, 9 November 2012. https://www.dazeddigital.com/artsandculture/article/15040/1/the-desert-of-the-unreal (Accessed 2/20/2020).

[9] The UAE's broader strategic program is known as the "UAE Centennial 2071" strategy, while Qatar's is the 2030 Vision development plan, launched in 2008.

technology market. The UAE's rapidly growing cybersecurity market was reportedly worth nearly half a billion US dollars in the summer of 2019.[10]

Since 2017, both Qatar and the UAE have increased domestic investments in the digital economy, most notably artificial intelligence (AI).[11] TRADOC Pamphlet 525-92 describes AI as possibly "the most disruptive technology of our time."[12] The AI national strategies of both Qatar and the UAE see it as a persistent feature of their domestic landscape in the near future. The UAE's strategy, for instance, envisions a future where AI is embedded in the fields of transport, health, space, renewable energy, water, technology, education, environment, and traffic. Qatari focus includes Arabic Language Processing, National Security (cybersecurity, advanced threat warnings), Precision Medicine and Systems Biology, Transportation and FIFA World Cup 2022, Food Security, Oil and Gas. The Qatari strategic plan's underlying "vision" is "to have AI so pervasive in all aspects of life, business and governance in Qatar

[10] The UAE's growing capabilities in the cyberdomain have been bolstered by a company called DarkMatter (https://www.darkmatter.ae). Established in 2014, by 2018 DarkMatter had a revenue of $400 million, with 80% of it reportedly coming from UAE government contracts. The company was founded by Faisal al-Bannai, who previously started a telecom retailer that became the largest in the Middle East (Axiom Telecom). He is the son of a high-ranking officer in the Dubai police. According to media reports, the company has enticed top cybersecurity expertise from their home governments with high salaries and generous benefits. An investigative news report from early 2019 documented how the UAE government, through DarkMatter and a further web of platforms and contractors, had hacked an iPhone used by the Qatari emir and targeted a range of opponents of the UAE government.

[11] In October 2017, the UAE released what it called its Strategy for Artificial Intelligence and appointed a new "Minister of State for Artificial Intelligence." The strategy is available here: http://www.uaeai.ae/en/. The AI strategy falls within a broader framework of the "UAE 2031 AI strategy" (https://ai-everything.com/uae-ai-2031-strategy/), which is mirrored by the "National Program for Artificial Intelligence" (https://ai.gov.ae/). Different emirates, most notably Dubai, also have their own strategies and programs, each with corresponding websites. The UAE's artificial intelligence efforts are broad and expansive, focused on a variety of sectors and overseen by several overlapping entities, most importantly the "Emirates Council for Artificial Intelligence and Digital Transactions" along with various other local and federal entities.
The lead in financing Qatar's Artificial Intelligence program is taken by the Qatar Foundation (QF) for Education, Science and Community Development, "a private, non-profit organization that is supporting Qatar's transformation from a carbon economy to a knowledge economy." In 2010, it established the Qatar Computing Research Institute (QCRI), one of the three specialized research centers in Hamad bin Khalifa University (https://www.hbku.edu.qa/en/qcri). Within the QCRI lies the Qatar Center for Artificial Intelligence (QCAI), which was established in the fall of 2018 and which published the country's "National Artificial Intelligence Strategy for Qatar" in early 2020.

[12] "The Operational Environment and the Changing Character of warfare," page 10.

that everyone looks up to Qatar as a role model for AI+X nation." "AI+X," according to the document, is shorthand for spaces where AI is "embedded in all aspects of human activity."[13]

AI is expected to transform cybersecurity. As a recent report from the World Economic Forum notes, "The battleground of the future is digital, and AI is the undisputed weapon of choice… one thing is clear: only AI can play AI at its own game."[14] Already, automated bot swarms are constantly on the prowl in Arabic-language social media conversations, seeking to influence discussions by silencing or amplifying certain narratives in order to shape trending topics and other metrics of what is on the mind of "the Arab street."[15] Differentiating between fake and real evidence is becoming increasingly difficult as AI-powered code is used to fabricate and promote content that is virtually indistinguishable from real documentary evidence, creating an information landscape in which passions and prior beliefs play more of a role in deciding what is "true" than objective evidence or accurate information.[16] As TRADOC pamphlet 525-92 argues, the convergence of these AI technologies, when used in a targeted fashion, "present the potential for devastating impact on nation-states' will to compete and fight."[17]

---

[13] "National Artificial Intelligence Strategy for Qatar," page 6. https://qcai.qcri.org/wp-content/uploads/2019/10/QCAI_MOTC_AI_Strategy_English_FINAL.pdf (Accessed 2/20/2020).

[14] "3 ways AI will change the nature of cyber attacks," *World Economic Forum*, 19 June 2019. https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/ (Accessed 2/20/2020).

[15] In the period surrounding the QNA attack, for instance, Marc Owen Jones explains how bot swarms were used "to manipulate Twitter trends, promote fake news, increase the ranking of anti-Qatar tweets from specific political figures, present the illusion of grassroots Qatari opposition to the Tamim regime, and pollute the information sphere around Qatar, thus amplifying propaganda discourses beyond regional and national news channels." Marc Owen Jones, "The Gulf Information War| Propaganda, Fake News, and Fake Trends: The Weaponization of Twitter Bots in the Gulf Crisis," *International Journal of Communication*, Vol 13 (2019). https://ijoc.org/index.php/ijoc/article/view/8994 (Accessed 2/20/2020).

[16] In the second half of 2019, both Facebook and Twitter suspended several accounts linked to Saudi Arabia, the UAE and Egypt, for engaging in "coordinated inauthentic behavior" (Facebook: https://about.fb.com/news/2019/08/cib-uae-egypt-saudi-arabia/ Twitter: https://blog.twitter.com/en_us/topics/company/2019/new-disclosures-to-our-archive-of-state-backed-information-operations.html). Qatari-aligned media regularly reports on these spambots, in part to contrast their self-presentation as Arabic-language pioneers in freedom of expression with their deceitful and manipulative opponents. See for instance: https://www.alaraby.co.uk/english/news/2019/9/20/twitters-removal-of-uae-spam-bots-are-not-enough

[17] "The Operational Environment and the Changing Character of warfare," page 23.

FUTURE TRENDS

Qatari-Emirati investments in the digital economy should continue growing, since the rulers of both countries consider the digital economy to be foundational to the future well-being of their societies. In contrast to resource extraction, which has sustained economic growth in both countries and in which ownership is for the most part delimited by national borders, the AI race is global and will exhibit a "winner takes all" dynamic where early movers will "accrue downstream benefits by owning the future 'means of production'."[18] Qatar, according to its National Artificial Intelligence Strategy, "is well positioned to take advantage of this golden opportunity and become a critical player in the AI economy of future," but given that the global competitiveness of the AI race, "we need to act with a sense of urgency to realize this opportunity before it becomes too late."[19] Similar sentiments are regularly expressed by Emirati officials and government documents.

An Emirati official recently described his country's future as follows: "If we want to draw a future perception of the UAE, years from now, we would see the features of the smart city where millions of devices and platforms are connected, producing massive amounts of data, many of which will be at risk of piracy or privacy violation."[20] As both Qatar and the UAE continue to digitize services, including public safety, the costs associated with sabotage or other forms of data tampering will increase. The importance of protecting the integrity of the systems will consequently grow, further driving growth in the cybersecurity market.[21] The importance to national security of safeguarding data in borderless cyberspace may also elicit a move to control the infrastructure on which information travels. A report by the UAE cybersecurity firm DarkMatter, for instance, argues for bringing the servers and other repositories of state

[18] "National Artificial Intelligence Strategy for Qatar," page 4.
[19] "National Artificial Intelligence Strategy for Qatar," page 14.
[20] "TRA Launches the UAE National Cybersecurity Strategy," *UAE Telecommunications Regulatory Authority*, 24 June 2019. https://www.tra.gov.ae/en/media-hub/press-releases/2019/6/24/tra-launches-the-uae-national-cybersecurity-strategy.aspx (Accessed 2/20/2020).
[21] Especially concerning in these countries will be the reliance on automated systems for water, as desalination and distribution systems become increasingly sophisticated, machine-controlled and outfitted with sensors. Threats to target critical infrastructure and other Internet-of-Things networks can be expected to increase.

information under territorial sovereign control: "DarkMatter observed that 102,750 of the 137,000+ websites under the .AE top-level domain are hosted outside territorial borders. The use of international webhosting services indicates that the majority of UAE organizations do not have complete sovereignty of their systems and information, which places sensitive data and operations at risk."[22] Similarly, Qatar's AI strategy notes how, when it comes to AI and national security, "highly strategic infrastructure should rely on homegrown and locally controlled solutions."[23]

Due to their miniscule native populations, Qatar and the UAE have historically relied on foreign talent to achieve a variety of developmental goals. While the digital economy will to some extent neutralize this disadvantage, the need for skilled labor remains, and in addition to offering expatriate workers high salaries and generous benefits, Qatar and the UAE have both established well-funded research centers, incubators, digital cities and a plethora of other institutions aimed at drawing in talent and developing the domestic digital industry, often in collaboration with foreign institutions focused on new technology. The UAE, for instance, recently established an AI-focused university that will cover all costs for its students.[24]

As control over data and information is increasingly viewed through the lens of national security, a reliance on close allies for sensitive cybersecurity matters may become more pronounced. At the same time, the need to move quickly in this "first-mover market" renders the quick procurement of technology a strategic market imperative. The UAE in particular has established a number of partnerships with Chinese companies, whose technology is often cheaper, better and less politically conditioned than Western technology.[25] Chinese implementation of AI-driven surveillance technologies provides a

[22] "Darkmatter Cyber Security Report June 2019." https://www.scribd.com/document/433531776/Darkmatter-Cyber-Security-Report-June-2019 (Accessed 2/20/2020).
[23] "National Artificial Intelligence Strategy for Qatar," page 12.
[24] "More than 3,000 apply to world's first AI university in Abu Dhabi," The National (UAE), 26 October 2019. https://www.thenational.ae/uae/more-than-3-000-apply-to-world-s-first-ai-university-in-abu-dhabi-1.928903 (Accessed 2/20/2020).
[25] Kai-Fu Lee, in discussing the differences between the US and China in terms of AI, points to four main factors that will determine AI supremacy: the amount of data available, the tenacity of entrepreneurs, the availability of

roadmap for countries seeking to implement new technologies on a vast scale; Qatar and the UAE are unique in that most of the potentially surveilled population is foreign and as such has less of a say in local government policy.[26] More broadly, so long as new technologies help maintain the domestic "ruling bargain" in which citizens exchange the right to political dissent for comfort and prosperity, nationals of both countries are unlikely to significantly oppose new-tech encroachments on their privacy.

The same technologies that empower surveillance methods also empower those seeking to circumvent or oppose them, and when it comes to government surveillance, hackers, privacy advocates and media outlets can together build a compelling narrative of how new technologies are being misused by adversary governments. Qatari media, which has positioned itself as a champion of political pluralism in other Arab countries, reports regularly on transgressions by the Emirati and Egyptian governments. The UAE has received extensive negative coverage from its use of software tools to track and surveil government critics beyond its borders.

Asymmetric responses to new surveillance tools, including simple measures such as using coded or hard-to-understand language to confound NLP-powered Internet monitoring and surveillance tools, are likely to become more widespread as governments increase their control over the cyber-information sphere.[27] This cat-and-mouse game will combine with innovations in automation and AI to make the information sphere more turbid. In Arabic-language social media, markers such as hashtags are already dominated by trolls and bot swarms seeking to manipulate opinions. This will further degrade the reliability of

well-trained scientists and a supportive policy environment. Broadly speaking, Lee believes that China has an advantage over the US. See: Lee, K. F. (2018). *AI superpowers: China, Silicon Valley, and the new world order*. Houghton Mifflin Harcourt.

[26] The UAE population is estimated to be slightly over 9 million, with slightly over 15% of them Emirati citizens. Qatari population is 2.6 million, with around 12% of them Qatari citizens.

[27] In Arabic-language social media, for instance, the growth of automated systems has led people to rely on dialectical and slang Arabic, which are harder for machines to master. Perhaps in a not too-distant future, two parallel spheres may coexist, with bots and public figures debating one another in standard Arabic in one, while actual humans stick to dialects and private languages for their exchanges on the other.

pronouncements regarding the "mood of the Arab street," which will more often than not actually be the "mood of the Arabic-enabled bot." A further consequence of AI permeating social media is increased volatility during social media dust-ups due to the speed at which automated systems can create, process and interpret information. A recent Twitter spat between Emirati- and Saudi-aligned groups over fighting in the Yemeni port city of Aden escalated so quickly that it required an intervention, by tweet naturally, from the ruler of Dubai.[28] The potential impact of targeted influence campaigns on major events such as the 2022 World Cup in Qatar or the Expo 2020 in Dubai is significant, and the narrative regarding these events will undoubtedly be fiercely contested.

The more worrisome cybersecurity scenarios involve attacks on critical infrastructure, which have grown in frequency since Stuxnet was uncovered in 2010.[29] Qatar and the UAE's reliance on the oil and gas industries for cash, along with their thirst for desalinated water and electricity, make them both vulnerable targets for critical infrastructure attacks, all the more so as these industries become increasingly automated. The UAE's Barakah nuclear plant, whose first reactor is expected to begin operating sometime in 2020, is the most prominent of the growing number of new potential targets for cybersabotage.

"Virtual wars," in Stefan Banach's formulation, play out in the form of "offensive and defensive cyber capabilities, social media, information operations (e.g. 'Fake News'), artificial intelligence, stealth

[28] "Qatar, UAE, Saudi Arabia: Competition in the Virtual Domain," *Foreign Military Studies Office OE Watch*, Vol. 9 Issue 10 (October 2019). https://community.apan.org/wg/tradoc-g2/fmso/m/oe-watch-past-issues/295386/download

[29] The 2012 Stuxnet malware targeted Iranian nuclear facilities. Since then, notable reported attacks include the Shamoon virus, which damaged thousands of computers at Saudi Arabia's Aramco in 2012, a 2012 malware attack on RasGas, Qatar's main natural gas company and a 2016 hack of the Qatar National Bank. The UAE experienced several threats as well, though none as prominent. For more see: By Dr. Tarek Cherkaoui, "Cyber-Conflict and the Gulf Crisis 2010-2017:A New Kind of Information Warfare?" *TRT World Research Center* (originally published in the journal "The Political Economy of Communication" Vol 6, No 1 (August 2018)). https://researchcentre.trtworld.com/images/files/reports/CyberWarfare.pdf (Accessed 2/20/2020).

technologies and cloaking techniques."[30] By this measure, Qatar and the UAE are increasingly involved in a virtual war that is above all focused on influencing perceptions on the global stage. To this extent, their targets are less one another than perceptions of one another in centers of power across the globe. In fighting this virtual war, both are becoming more capable at shaping how populations and leaders in foreign countries interpret and engage with the Arabic-speaking world. Increasing their capabilities in this domain gives them leverage not only over one another but also, to some degree, over the foreign countries themselves.

[30] Stefan J. Banach, "Virtual War – A Revolution in Human Affairs," *Small Wars Journal*, https://smallwarsjournal.com/jrnl/art/virtual-war-revolution-human-affairs (Accessed 2/20/2020).