Combined Air Operations Center at Al Udeid Air Base, Qatar, provides command and control of airpower throughout Iraq, Syria, Afghanistan, and 17 other nations (U.S. Air Force/ Joshua Strang)

Political Warfare with Other Means

2017 Cyber Attacks on Qatar

By Edwin Y. Chua

It's one of the great paradoxes of our time that the very technologies that empower us to do great good can also be used to undermine us and inflict great harm.

—President Barack Obama

On May 24, 2017, Qatar's state news agency reported that Qatari Emir Tamim bin Hamad Al Thani supported Hamas, Hizballah, Iran, and Israel.[1] In response, Saudi Arabia, the United Arab Emirates (UAE), Bahrain, and Egypt cut off relations with Qatar, a fellow member of the Gulf Cooperation Council (GCC).[2] The four countries released a list of 13 demands that aimed to align Qatar's national policies with that of other Gulf and Arab countries.[3] However, Qatar's state news agency quickly disavowed the report on its Web site and Twitter account and attributed it to a cyber attack.[4] The attack on Qatar's state news agency to promulgate false and misleading information marks a new phase in the use of cyber means for political warfare. An analysis of the goal, target audience, and means of this cyber attack, as well as the results of the attack and the implications of evolving technologies, suggest that defending against such attacks requires a multifaceted effort from individuals, organizations, governments, and the international community.

Political analyst Graham Fuller, a former vice chairman of the National Intelligence Council at the Central Intelligence Agency, postulates that the aim of the 2017 cyber attacks was to compel Qatar to align its foreign policy

Major Edwin Y. Chua, Singapore Army, wrote this essay while a student at the Marine Corps Command and Staff College. It tied for first place in the Strategy Article category of the 2018 Chairman of the Joint Chiefs of Staff Strategic Essay Competition.

with Saudi Arabia, end its good relations with Iran, cut off military ties with Turkey, and terminate its support for al Jazeera news network.[5] Qatar has close diplomatic ties with Iran because they jointly exploit the South Pars natural gas fields.[6] In 2014, Qatar signed a defense agreement with Turkey and agreed to allow Turkey to establish a military base in Qatar.[7] Fuller explains that these international ties allowed Qatar to chart its own foreign policy independent of Saudi Arabia. In the aftermath of the Arab Spring, which threatened the rule of authoritarian leaders in the region, many Arab leaders saw al Jazeera's news channels as threatening to their control of information in the region.[8] The target audience of the cyber attack was not only the political elites in Qatar, but also the leaders of other countries in the GCC (that is, Kuwait and Oman) and key decisionmakers in the United States. By highlighting Qatar's close ties with Iran and Hamas, a U.S.-designated terrorist group, the bogus news reports aimed to politically isolate Qatar from the United States. The other GCC states were expected to rally along religious lines to support the Saudi coalition, which adheres to the Sunni branch of Islam, against Iran, a Shiite state.

To reach these audiences, the UAE, as part of the Saudi coalition, enacted a program of cyber attacks into Qatar's state news agency to insert false news reports. Hackers began their operation in April 2017, gaining total control of the Qatari News Agency's network, email accounts, Web sites, and social media platforms.[9] This control was used to disseminate false information from May 24 to May 25, before the state media's information technology experts were able to regain control.[10] The cyber attacks supported a broader campaign that included all elements of national power including diplomatic, military, and economic efforts. After the attack, the Saudi coalition severed diplomatic ties and gave Qatari citizens 14 days to leave their territory while banning their own citizens from traveling to or residing in Qatar.[11] Under diplomatic pressure from Saudi Arabia, countries such as Yemen, Maldives, and Libya severed their diplomatic ties with Qatar.[12] The Saudi coalition also closed their airspace to Qatari aircraft and banned all ships flying the Qatari flag or serving Qatar from docking at any ports.[13] Saudi Arabia closed Qatar's only land border as well.[14] These efforts on land, sea, and air aimed to cut off Qatar's supply routes and threaten its economy.

Less Than Success

Despite the use of all elements of national power, the Saudi coalition did not succeed in achieving its aim of isolating Qatar from the GCC and the United States. Qatar did not give in to the 13 demands presented by the coalition.[15] In the immediate aftermath, the U.S. Secretary of State called for the crisis to be resolved diplomatically, while the U.S. Department of Defense and Ambassador to Qatar publicly praised Qatar for hosting the al Udeid Air Base and its commitment to regional security.[16] Kuwait and Oman, the other two members of the GCC, did not cut off their diplomatic ties with Qatar. Less than a month after the hacks against Qatar, U.S. intelligence officials attributed the cyber attack to the UAE and stated that the attacks had been directed by senior members of its government.[17] The land, sea, and air blockades did not have a significant impact, as Turkey and Iran sent food and basic supplies directly to Qatar.[18] Turkey also sent more military forces to its base in Qatar in order to deter any Saudi military action.[19] The failure of this cyber attack, despite the close coordination of all instruments of national power, supports the theory posited by some cybersecurity researchers that states using cyber attacks rarely achieve their intended objectives, and successful compellence could require the overwhelming national power of countries like the United States.[20]

However, while the ploy to isolate Qatar was exposed, there has not been any public censure or consequences to the UAE for its conduct of the cyber attacks. The lack of consequences for the UAE could set a precedent and embolden future adversaries to leverage cyber attacks in support of political warfare. The proliferation of such attacks could indicate that the "strategic logic of cyber is shifting to one of disruption and constant harassment designed to signal capability and the threat of escalation."[21]

Looking Forward

Future cyber attacks and information operations would exploit the development of software that could manipulate voice and video. In November 2016, Adobe, a company known for its Photoshop software, unveiled Project VoCo, a program that makes it possible to take an audio recording and alter it to include words and phrases that the original speaker did not say, in the voice of the original speaker.[22] Another company, BabelOn, is developing software that can translate a person's voice into another language instantly.[23] Researchers at the University of Washington are experimenting with the use of artificial intelligence (AI) to convert audio files into realistic mouth movements, which could be used to falsify videos of public personalities giving speeches.[24] The widespread use of such technologies would blur the lines between truth and falsehood, allowing malicious actors to conduct a persistent campaign of distortion to smear the reputation of certain world leaders or countries in order to reduce their soft power and influence over time.

A strong, multifaceted defense is needed against the abuse of such new software and AI. This defense will require action by individuals, organizations, governments, and the international community. Adobe's acknowledgment of the potential abuse of its software is a good step toward building public awareness to inoculate individuals against insidious influence campaigns. More effort should also be focused on developing software that can detect such voice and video manipulation quickly. Learning from the experience of Qatar, governments and organizations should be prepared to embrace transparency and quickly report cyber attacks when they occur to shape the narrative, clarify the position of the government or organization, and prevent

the spread of distorted information. Governments and organizations should also be consistent in their public outreach efforts to prevent any misunderstandings from being exploited during a crisis through the use of fake photos, videos, or sound recordings. One example of this can be seen in the Summary of the 2018 United States National Defense Strategy, which calls on the United States to be "strategically predictable" in demonstrating its commitment with allies to deter aggression.[25] Additionally, there should be an increased effort to strengthen international norms against such forms of cyber attack and to increase the costs to countries conducting such attacks. The NATO Cooperative Cyber Defense Center of Excellence in Estonia, which has released two Tallinn Manuals on cyber conflict, is one such organization that could help to develop such cyber norms.[26]While the cyber attacks on Qatar were ultimately unsuccessful, they marked a new use of cyber means to distort information. This use of cyber means could become increasingly common, especially as technological advances make it easier to conduct such attacks and falsify or distort information, and the risks and downsides of being caught remain low. The United States should build public awareness of such threats, enhance its public diplomacy efforts as a preemptive measure, and leverage its allies and partners in the international effort to establish norms against such activities. It should also censure the countries conducting such activities, when appropriate. This preemptive approach will establish norms for the appropriate use of cyber and contribute to the protection of the United States and its allies. JFQ

Notes

[1] Bethan McKernan, "Qatar Accuses UAE of Violating International Law by Hacking State News Agency," *Independent*, July 17, 2017, available at <www.independent.co.uk/news/world/middle-east/qatar-uae-international-law-hacking-news-agency-al-jazeera-cyber-attack-gulf-united-arab-emirates-a7845456.html>.

[2] Alex Shanahan, "U.S. Role, Stake in Gulf Feud," *Washington Report on Middle East Affairs* 36, no. 5 (August–September 2017), 46.

[3] "Arab States Issue 13 Demands to End Qatar-Gulf Crisis," Al Jazeera, July 12, 2017, available at <www.aljazeera.com/news/2017/06/arab-states-issue-list-demands-qatar-crisis-17062 3022133024.html>.

[4] "Foreign Minister: 'Qatar Will Address the Media Campaign Targeting It,'" Qatar Ministry of Foreign Affairs News, May 25, 2017, available at <https://mofa.gov.qa/en/all-mofa-news/details/2017/05/25/foreign-minister-%27qatar-will-address-the-media-campaign-targeting-it%27>.

[5] Graham E. Fuller, "Does Qatar Really Threaten the Gulf?" *Washington Report on Middle East Affairs* 36, no. 5 (August–September 2017), 20.

[6] "Qatar-Iran Ties: Sharing the World's Largest Gas Field," Al Jazeera, June 15, 2017, available at <www.aljazeera.com/indepth/interactive/2017/06/qatar-north-dome-iran-south-pars-glance-lng-gas-field-170614131849685.html>.

[7] "President Erdogan Visits Turkey Military Base in Qatar," *Hurriyet Daily News* (Istanbul), November 16, 2017, available at <www.hurriyetdailynews.com/president-erdogan-visits-turkey-military-base-in-qatar-122498>.

[8] Fuller, "Does Qatar Really Threaten the Gulf?" 20.

[9] "Qatar Says Cyberattack 'Originated from the UAE,'" Al Jazeera, July 20, 2017, available at <www.aljazeera.com/news/2017/07/qatar-sheds-light-cyberattack-official-media-170720151344996.html>.

[10] Karen DeYoung and Ellen Nakashima, "UAE Orchestrated Hacking of Qatari Government Sites," *Washington Post*, July 16, 2017, available at <www.washingtonpost.com/world/national-security/uae-hacked-qatari-government-sites-sparking-regional-upheaval-according-to-us-intelligence-officials/2017/07/16/0c46e54-698f-11e7-8eb5-cbccc2e7bfbf_story.html?utm_term=.fef1e4846f4a>.

[11] "Qatar Crisis: What You Need to Know," BBC, July 19, 2017, available at <www.bbc.com/news/world-middle-east-40173757>.

[12] Noah Browning, "Arab Powers Sever Qatar Ties, Citing Support for Militants," Reuters, June 5, 2017, available at <www.reuters.com/article/us-gulf-qatar/arab-powers-sever-qatar-ties-citing-support-for-militants-idUSKBN18W0DQ>.

[13] "Qatar Crisis: What You Need to Know."

[14] Ibid.

[15] "Qatar Crisis: Saudi-Led Coalition Drops 13 Demands to End the Boycott," *Haaretz* (Tel Aviv), July 19, 2017, available at <www.haaretz.com/middle-east-news/qatar-crisis-saudi-led-coalition-drops-13-demands-to-end-the-boycott-1.5431407>.

[16] "Tillerson Says Break with Qatar by Saudi Arabia, Others Won't Affect Counter-Terrorism," CNBC, June 5, 2017, available at <www.cnbc.com/2017/06/05/tillerson-says-break-with-qatar-by-saudi-arabia-others-wont-affect-counter-terrorism.html>; DeYoung and Nakashima, "UAE Orchestrated Hacking of Qatari Government Sites"; and Phil Stewart, "U.S. Military Praises Qatar, Despite Trump Tweet," Reuters, June 6, 2017, available at <www.reuters.com/article/us-gulf-qatar-usa-pentagon/u-s-military-praises-qatar-despite-trump-tweet-idUSKBN18X2G2>.

[17] DeYoung and Nakashima, "UAE Orchestrated Hacking of Qatari Government Sites."

[18] "Iran, Turkey Send Food to Qatar Amid Fears of Shortages," Voice of America, June 11, 2017, available at <www.voanews.com/a/tillerson-cavusoglu-qatar/3895653.html>.

[19] "How Turkey Stood by Qatar Amid the Gulf Crisis," Al Jazeera, November 14, 2017, available at <www.aljazeera.com/news/2017/11/turkey-stood-qatar-gulf-crisis-171114135404142.html>.

[20] Brandon Valeriano, Ryan C. Maness, and Benjamin Jensen, *Cyber Strategy* (New York: Oxford University Press, forthcoming), 111.

[21] Brandon Valeriano, Ryan C. Maness, and Benjamin Jensen, "Cyberwarfare Has Taken a New Turn: Yes, It's Time to Worry," *Washington Post*, July 13, 2017, available at <www.washingtonpost.com/news/monkey-cage/wp/2017/07/13/cyber-warfare-has-taken-a-new-turn-yes-its-time-to-worry/?utm_term=.474c4314fa45>.

[22] Matthew Gault, "After 20 Minutes of Listening, New Adobe Tool Can Make You Say Anything," *Motherboard*, November 5, 2016, available at <https://motherboard.vice.com/en_us/article/jpgkxp/after-20-minutes-of-listening-new-adobe-tool-can-make-you-say-anything>.

[23] Nathan Ingraham, "BabelOn Is Trying to Create Photoshop for Your Voice," *Endgadget*, June 22, 2017, available at <www.engadget.com/2017/06/22/babelon-is-trying-to-create-photoshop-for-your-voice/>.

[24] James Vincent, "New AI Research Makes It Easier to Create Fake Footage of Someone Speaking," *TheVerge*, July 12, 2017, available at <www.theverge.com/2017/7/12/15957844/ai-fake-video-audio-speech-obama>.

[25] *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 2018), 5, available at <www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

[26] "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations to Be Launched," NATO Cooperative Cyber Defence Centre of Excellence, February 2, 2017, available at <https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html>.