QATAR-AMERICA INSTITUTE

Briefing Report

Cyber Attack on the Qatar News Agency

Fake News, Cyber War, and an Attack on International Norms of Sovereignty

By Mike Sexton, Fellow at the Qatar-America Institute

Executive Summary

- Starting April 19, hackers successfully used VPNs, exploits, and malware to penetrate the website, Twitter, and YouTube pages of the Qatar News Agency (QNA).
- Fabricated quotes from High Highness Sheikh Tamim bin Hamad al-Thani, Emir of Qatar, and Mohammed bin Abdulrahman bin Jassim al-Thani, Qatari Minister of Foreign Affairs were posted on the hacked Twitter page and website of QNA at 12:13am Wednesday May 24, 2017.
- Traffic logs indicate a spike in visits – anomalous for the late hour – from certain IP addresses in a fellow GCC country in the hour preceding the publication of the fabricated quotes.
- Immediately after publication, the fabricated quotes became major news in two other GCC countries. Over 20 political figures and senior guests were promptly available – between 1am and 5:30am local time – to discuss the fabricated quotes and criticize the Qatari government on live television in the two countries.
- Within 45 minutes of the fabricated quotes' publication, the Qatari government notified regional media broadcasters of the cyber attack and falsity of the quotes. Media outlets in the two other GCC countries, however, ignored the alert and continued broadcasting the fabricated quotes.
- A week and a half later, certain Arab countries began severing diplomatic relations with Qatar. Their airspace was restricted to Qatari flights, borders were closed restricting food shipments, and access to Qatari news sources was blocked in their countries.

Background

Qatar News Agency

The Qatari government established the Qatar News Agency (QNA) in 1975 covering local news – the second such Arab news agency covering the Gulf region. In contrast to the more recently established Al Jazeera, QNA's audience is much smaller, and primarily domestic. As a result of QNA's relatively small size, anomalous patterns in the volume and origin of traffic on QNA's website are much more pronounced.

QNA is a highly reputable news source, accredited by the Arab News Agency Union, and having presided over the Federation of Arab News Agencies (FANA) for two years, contributing to the development of Arab news media sources.[1] QNA features news stories in Arabic and English.[2]

The North Camp Square Graduation

On May 23, 2017, 7–9am Doha time, Sheikh Tamim bin Hamad al-Thani, Emir of Qatar, witnessed the graduation ceremony of the eighth class of national service conscripts. The event was widely attended, with the audience including ministers, senior military leaders, and the Defense Attaches of the United States and United Kingdom.

HH Sheikh Tamim bin Hamad al-Thani gave no remarks at the graduation ceremony. The full two-hour ceremony was broadcast live, recorded, and is available to view on YouTube.[3]

The QNA Cyber Attack

At 12:13am local time on May 24, 2017, the Qatar News Agency website and Twitter and YouTube accounts were hacked to publish that the Emir made several controversial comments on Qatar's foreign relations at the graduation ceremony. The fabricated quotes included:

- That Qatar's relations with the Trump administration were "tense" and that President Trump is unlikely to stay in office for long[4]
- That Iran is an "Islamic power" and "a big power in the stabilization of the region"
- That Hamas is "the legitimate representative of the Palestinian people"
- That relations with Israel are "good"[5]

The reported quotes were not only fabricated but also positively disprovable from the footage of the event. Despite this, articles from other Gulf news outlets like Saudi-owned Al Arabiya still treat the reports of fabricated quotes of the Emir as credible.[6]

[1] *https://web.archive.org/web/20161130142348/http://www.qna.org.qa/en-us/AboutQNA/Vision*

[2] *https://www.webcitation.org/5wTqoKwQM?url=http://www.mondotimes.com/1/world/qa/241/all/12247*

[3] *https://www.youtube.com/watch?v=KOSyLFraa2I*

[4] *https://www.independent.co.uk/news/world/middle-east/qatar-news-agency-fake-news-israel-praise-criticise-allies-middle-east-sheikh-donald-trump-a7753026.html*

[5] *http://www.foxnews.com/world/2017/05/23/qatar-says-state-news-website-hacked-fake-article-published.html*

[6] *https://english.alarabiya.net/en/News/gulf/2017/05/24/Qatar-says-Iran-an-Islamic-power-its-ties-with-Israel-good-.html*

Timeline of the Cyber Attack

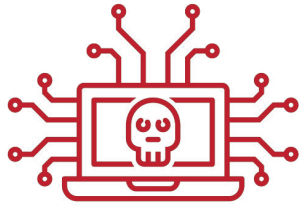
April 19:	A hacker utilizing a virtual private network (VPN) infiltrated QNA's network and scanned the QNA website.
April 22:	The hacker exploited a vulnerability in QNA's website to install malware and further penetrate the network. Another user received the vulnerability and accessed it at 5:47am – using the same IP address as one used to plant the fake news story on May 24.
April 22-28:	The hacker installed more sophisticated malware to escalate control of the QNA network.
April 28:	The hacker targeted and collected the internal email addresses and passwords of QNA employees, then shared them with another user via Skype.
May 20:	The hacker reestablished access to the QNA network using the malware, presumably in preparation of the attack.
11pm May 23 - 12:13am May 24:	QNA's website sees an anomalous late-night surge in traffic from certain IP addresses in one of the siege countries, suggesting foreknowledge of the attack.
12:13am May 24:	The false quotes from Emir Tamim bin Hamad al-Thani were posted on the QNA website.
12:15am May 24:	The article is first accessed by an IP address in one of the siege countries. The website soon received a dramatic surge in traffic, including 86 visits in thirty minutes from just two or three apparent individuals from IP addresses in the siege countries. The traffic surge overwhelmed the host system and knocked it offline.
12:15am – 5:30am May 24:	State news channels and websites in two other GCC countries immediately begin broadcasting and publishing the fabricated story, with 20 senior guests available to discuss the (false) report. This continued despite the Qatari Government Communications Office GCO releasing a statement at 2am announcing that QNA had been hacked and that the reported quotes were fabricated. The statement from the GCO was acknowledged and heeded by virtually all news outlets except those in the two other GCC countries.
3am May 24:	QNA contained the hack and restored access to the website.
Morning, May 24:	Agence France Press, Associated Press, Reuters reported on the cyber attack against QNA – referring to the reported quotes as a component of the hack and not as credible statements.
4:49pm, May 24:	Qatar's Ministry of Foreign Affairs released a statement reaffirming that QNA was hacked, stating that an investigation into the attack was beginning, and expressing concern at foreign media outlets continuing to treat the reported quotes as genuine.
May 24 (throughout):	Saudi Arabia and the United Arab Emirates began blocking Qatari news sources within their countries.

7pm May 24:	QNA recovered access to all its social media accounts.
12pm May 25:	HE the Qatari Foreign Minister Mohammed bin Abdulrahman al-Thani released a statement announcing the coordinated campaign targeting Qatar and its media and underscoring Qatar's desire to maintain good relations with the GCC.
May 28:	The UAE's Foreign Minister Abdullah bin Zayed al-Nahyen stated that "Qatar's behavior threatens stability in the Gulf."
June 5:	Saudi Arabia, Bahrain, the UAE, and Egypt sever diplomatic relations with Qatar.

Information and Cyber Warfare

The cyber attack on the Qatar News Agency is an attack not just on Qatar, but on international norms of sovereignty and on truth itself. The attack is a historic case of both cyber and information warfare, and treating it as such is critical to deterring comparable operations in the future. If not, similar efforts – like foreign interference in the 2016 U.S. presidential election will only become more commonplace.

In 2016, foreign intelligence agents made a concerted effort to manipulate American public opinion in the midst of an election by hacking into the networks of political officials, strategically leaking ill-gotten secrets to manipulate the media environment, and proactively disseminating fabricated news stories to provoke outrage. The interference may not have constituted a violation of international law, but it was uncontroversially understood to be a brazen violation of U.S. sovereignty and was condemned and punished accordingly. Deterring similar cyber and information warfare attacks in the future will be profoundly challenging – and failing to address attacks like that on QNA will only make it more difficult.



Qatar's predicament, thus, is inextricable from the United States' own challenge to maintain international norms and order. Failing to sufficiently hold the perpetrators accountable will signal to other unscrupulous states that they can conduct similar attacks to sway elections or instigate diplomatic conflicts in the future. It is imperative that the United States and international community unequivocally signal that these attacks are illegitimate exercises of state power and that diplomatic conflicts that arise as a result will be handled accordingly.

International Law

In 2013, the NATO Cooperative Cyber Defence Centre of Excellence published an academic study known as the "Tallinn Manual," exploring how international legal concepts like jus ad bellum applied to cyberspace. The Tallinn Manual asserts that the classical notion of state sovereignty applies to cyberspace, stating that "States may exercise sovereign prerogatives over any cyber infrastructure located on their territory,"[7] and

[7] *https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf (pg. 16)*

that, "[a] cyber operation by a State directed against cyber infrastructure located in another State may violate the latter's sovereignty."[8] This notion would likely imply that the cyber attack on the Qatar News Agency – which is not only located in but owned by Qatar – violated the sovereignty of Qatar. While the Tallinn Manual is not a binding legal document, it is a well-accepted work of legal analysis and can realistically inform how the international community treats malicious activity like the QNA cyber attack.

The corpus of international law vis-à-vis cyberspace is notoriously limited, forcing states to take an ad hoc approach to punishing and deterring malicious activity like disruption of the 2016 US presidential election or the cyber attack on Sony Pictures. Because of differences in opinion on matters like free speech online and cyber espionage, it is challenging to forge a consensus between states around what sort of actions in cyberspace should be considered off limits. The fact that an unauthorized individual deliberately and maliciously accessed the QNA network would make the cyber attack an unambiguous violation of the Computer Fraud and Abuse Act in the United States;[9] in international law, however, cyber law primarily inherits the consequences of the Law of Armed Conflict (LOAC).[10] According to homeland security expert and legal scholar Paul Rosenzweig, the profound difference between the effects of armed conflict and cyber conflict make the application of LOAC principles to cyber conflict "in the mid-to-long term… unsustainable."[11]

The inadequacy of international law to address the cyber attack on the Qatar News Agency should not lead the international community to allow it to go unanswered. The well-established sovereignty of the state of Qatar has been deliberately violated. That violation of sovereignty, furthermore, is now being cynically exploited as pretense for a historic diplomatic siege. It would be a travesty of justice for mediators of the diplomatic crisis to not account for the morally indefensible cyber attack that precipitated it.

[8] *https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf (pg. 16).*
[9] *https://www.law.cornell.edu/uscode/text/18/1030*
[10] *http://www.genevacall.org/wp-content/uploads/dlm_uploads/2013/11/The-Law-of-Armed-Conflict.pdf*
[11] *https://www.lawfareblog.com/new-face-law-and-cyber-warfare*

Some information contained in this report was sourced directly from the State of Qatar.