



THE INVESTIGATIVE JOURNAL
— TRUTH IN JOURNALISM —

THE STATE OF QATAR'S HACK OF OUR DEMOCRACIES

—
Richard Miniter

2019





BREACHED: Sony Pictures' California HQ suffered a cyberattack in 2014, thought to originate with North Korea's attempt to block a film satirizing Kim Jong-un (REUTERS)

Introduction

In one of the largest state-sponsored computer hacks ever detected, Qatar's proxies cyberattacked more than 1,400 high-status and ordinary citizens who were exercising their free-speech rights in democracies across North America, the Middle East and Europe, according to U.S. court filings, computer-forensic reports and expert testimony provided in pre-trial motions.

The targets included current and former U.S. government officials, ambassadors and United Nations officials, as well as actors, international soccer players, activists, executives, fundraisers, diplomats, generals, dissidents, scholars, journalists, rabbis and imams from around the world. Even members of royal families and heads of state — e.g. Bahrain's Crown Prince Salman bin Hamad al-Khalifa and United Arab Emirates' (UAE's) Her Highness Sheikha Hind Bint Maktoum Bin Juma al Maktoum (wife of Dubai's ruler and niece of HH Sheikh Mohammed bin Rashid al Maktoum) — were among those affected.

The list of prominent Middle Eastern, European and North American targets also included:

Sami Hafez Anan, Egypt's former Chief of the General Staff of the Armed Forces; Secretary-General of the Arab League and former Egyptian foreign minister Ahmed Abdul Gheit; Assistant Secretary-General of the Arab League and former Egyptian ambassador Hossam Zaki; UAE official and diplomat Sheikh Maktoum Bin Bhutti al Maktoum; Saudi Arabian Minister of State for African Affairs and former Egyptian ambassador Ahmed Abdul Aziz Kattan; Egyptian Cabinet Member and Minister of State for Foreign Affairs Mohammed Gargash; Wolfgang Pusztai, security and policy analyst, and former Austrian defense attaché; James Lamond, managing director and senior policy adviser at the

Center for American Progress, and former director at Glover Park Group; American Rabbi Shmuley Boteach; and Kristin Wood, former senior analytics adviser at the Open Source Center, Central Intelligence Agency, who led the Terrorism Analysis team examining al-Qaeda's ties to Middle Eastern countries at the Counterterrorism Center (CTC).

At a time when the U.S. media has been consumed by speculation about Russian interference in its 2016 presidential elections, and Hollywood is still reeling from North Korea's computer attacks on Sony Pictures,¹ the depth of Qatar's digital strikes has gone largely unrecognized. Here the details of the hack are revealed in full for the first time.

1. <https://www.independent.co.uk/life-style/gadgets-and-tech/news/north-korea-hackers-server-thailand-sony-pictures-cyber-attack-a8329586.html>

Qatar's Cyber War: The Background

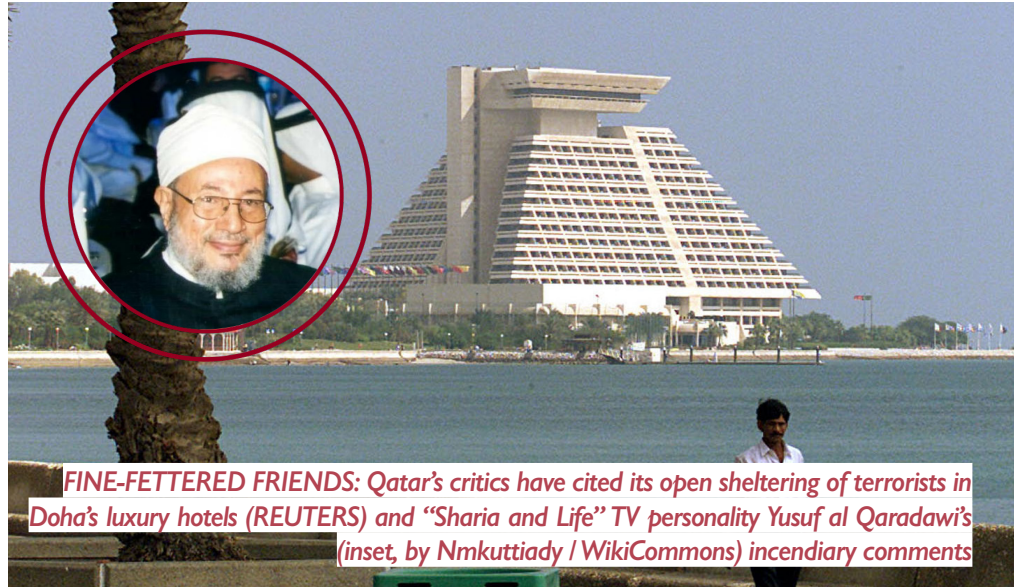
Qatar's computer warfare is unprecedented in its duration (stretching over a four-year period from 2014–2018), geographic reach (including attacks on victims in three continents — Asia, Europe and North America), and scope (afflicting more than 1,400 people).

And although they are united in the effects of these attacks, the victims have no other personal or professional ties to each other, apart from the remarks they have made that were publicly critical of Qatar.

These critics of the Qatari regime were engaging their constitutionally protected rights to speech rights within the Western democracies or countries they hail from when their offending remarks were made. They cited Qatar's open, traceable and public financial support for the Muslim Brotherhood and Hamas — designated as a terrorist group by the U.S., the EU, Canada and Israel — and the Qatari government's use of its *Al Jazeera* broadcasts to normalize terrorist viewpoints.

“

Qatar's shocking hack reveals the blueprint rogue nations can use to target ordinary citizens, topple politicians and subvert political movements in the open societies they oppose. Democracy's silent enemy now lurks on every citizen's smartphone, tablet and laptop”



They also mentioned Qatar's harboring of Hamas and other terrorist leaders inside luxury hotel complexes² within the Qatari capital, Doha. In other words, the country's critics and the targets of its hacking operations only cited information that is publicly available and undisputed.

Yet the accuracy of the criticism is not in doubt.

Qatar has officially acknowledged its financial support for Hamas³ and its support for the Muslim Brotherhood.⁴

Any review of *Al Jazeera's* Arabic-language broadcasts will reveal that Yusuf al Qaradawi,⁵ the Brotherhood's spiritual guide, had a weekly show called "Sharia and

Life"⁶ for years, which was watched by millions of viewers and on which he still appears as a guest.⁷

During one of his controversial appearances as a studio guest, he was asked by the anchor if he supported suicide bombings in Syria. An impassioned Qaradawi shamelessly responded that jihadists should not blow themselves up unless the operation is endorsed by the Brotherhood.

The Middle East Research Institute (MEMRI),⁸ a non-profit group that monitors Arabic-language media and translates its output, has presented many examples of *Al Jazeera's* presenting pro-terrorist viewpoints.

Alberto Fernandez, vice president of MEMRI, offered this balanced assessment: "My personal views on *Al Jazeera* are complicated, even though it is obvious that much of its content is deeply disturbing.

2. https://www.washingtonpost.com/news/worldviews/wp/2017/06/23/why-saudi-arabia-hates-al-jazeera-so-much/?u&utm_term=.5a37717d3d66

3. <https://www.haaretz.com/middle-east-news/qatar-vowes-to-continue-supporting-hamas-in-gaza-1.5493246>

4. <https://www.theatlantic.com/international/archive/2017/07/muslim-brotherhood-qatar/532380/>

5. https://en.wikipedia.org/wiki/Yusuf_al-Qaradawi

6. https://www.washingtonpost.com/news/worldviews/wp/2017/06/23/why-saudi-arabia-hates-al-jazeera-so-much/?u&utm_term=.58030dc38e71

7. <https://www.aljazeera.com/programmes/whatkilleddarafat/2012/07/2012732069963178.html>

8. <https://www.memri.org>

9. <https://www.memri.org/reports/defending-and-attacking-mythological-version-al-jazeera-television>



MIXED MESSAGES: Staff at work inside Al Jazeera's Doha HQ, June 2017. The Qatari-owned network both transmits and elicits conflicting views (REUTERS)

“The truth of *Al Jazeera* is rather more than those who want to shut it down and those who defend it. It is BOTH a legitimate, historically important news operation, and an open and constant exercise in Islamist agitprop,” continues Fernandez. “[Islamic scholar] Fouad Ajami perfectly captured the tone and nuance of the station in 2011 when he noted that, ‘day in and day out, *Al Jazeera* deliberately fans the flames of Muslim outrage.’”¹⁰

Living as they did in free, democratic countries, Qatar’s critics had every reason to expect that their nations’ laws and traditions would safeguard their rights to speak freely. Now Qatar’s hacks have changed those expectations.

“If true — and the story seems to be strongly corroborated — it would constitute a dangerous and direct attack by a foreign government against American citizens for exercising their First Amendment rights,” American Rabbi Shmuley Boteach said in a statement to *Breitbart*.¹¹

“It would constitute an assault against a Rabbi and his wife, a mother of nine, for speaking out against the Jewish lobbyists who took millions

of dollars to help cleanse Qatar of its terror-funding record.”

Still, Qatar’s leaders appeared to be alarmed that critics might shift U.S. or EU policy against the gas-rich peninsula. These fears also have a strong basis in fact. Indeed, some American critics who were hacked, such as American Rabbi Shmuley Boteach, had called for changes to U.S. policy, including shuttering the U.S. military base in Qatar and taking a harder line against the country.

So, Qatar apparently authorized a wide-ranging hack and attack on its international critics, as court documents show.¹²

Clearly, intelligence officials say, the West is entering a new era of asymmetric warfare. Nations that cannot hope to challenge the U.S. or NATO on any traditional battlefield are using the Internet — an information superhighway originally built by the U.S. military itself — to wage war on the superpower.

“On September 11th, terrorists used our own civilian airplanes against us,” said a former

U.S. Navy Seal and CIA contractor, who sought anonymity given his past field work. “Now they are using our own Internet against us.”

Qatar’s shocking hack deserves a closer look because it reveals the blueprint that rogue nations can use to target ordinary citizens, topple politicians and subvert political movements in the open societies they oppose. Democracy’s silent enemy now lurks on every citizen’s smartphone, tablet and laptop.

“
If true, this would constitute a dangerous and direct attack by a foreign government against American citizens for exercising their First Amendment rights”

—Rabbi Shmuley Boteach



10. <https://www.nytimes.com/2001/11/18/magazine/what-the-muslim-world-is-watching.html>

11. <https://www.breitbart.com/politics/2018/09/18/qatar-targeted-rabbi-shmuley-wife-with-hacking-attacks-report/>

12. See PDF attached / in online article link

How Oil and Gas Gave Rise to Qatar's Power

Qatar is a small arm of land, roughly the size of the state of Connecticut, which reaches out some 160km (100 miles) into the Arabian Gulf. It has been ruled by the Al Thani dynasty since 1825, with various degrees of autonomy under Ottoman Turkish and British imperial rules.

Technically independent after World War I, in practice Qatar became a British Trucial State in 1916 following the Allied victory in “the war to end all wars.” When British explorers found high-quality oil and gas there in 1940, the Qatar Petroleum Company¹³ was formed, resulting in the emirate’s slow transformation from a colonial waystation largely populated by fishermen, herders and traders with a way of life little changed since the peninsula’s Neolithic origins into a modern superpower offering a strategic energy source.

By 1949, Qatar was exporting its petroleum products to Europe. To this day, energy sales remain the emirate’s largest source of income. As the British retreated from the Middle East, yielding modern-day Bahrain and other



POWER WALK: Qatari Emir Sheikh Tamim bin Hamad al-Thani arriving at Bole International Airport, Addis Ababa, Ethiopia, 2017 (REUTERS)

Gulf emirates in the 1960s and 1970s, Qatar secured full independence from the crown in 1971. The Al Thani

clan has continued to rule.

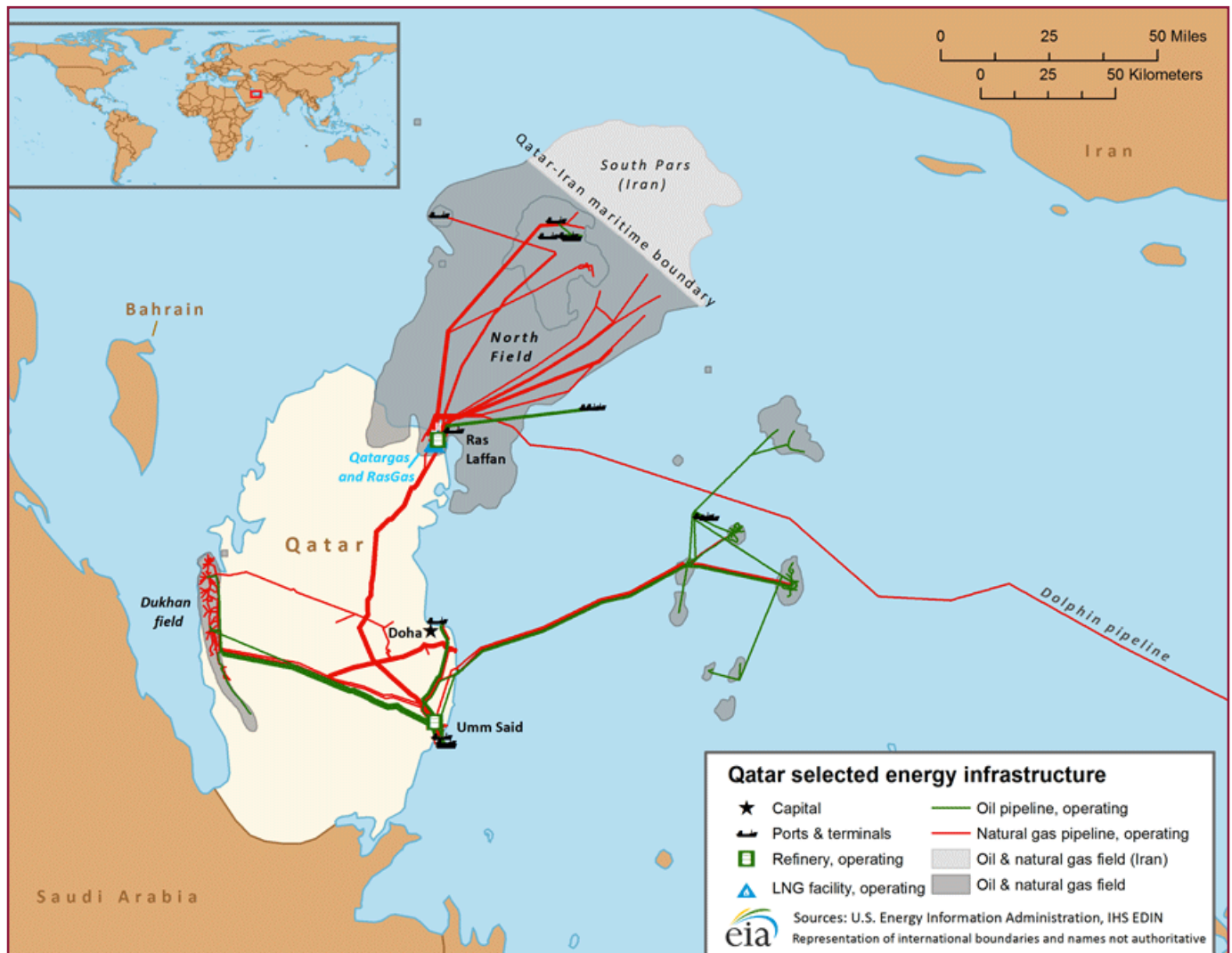
Since gaining independence, Qatar has discouraged opposition political parties and has dealt firmly, even with peaceful dissidents. Its people have little say in setting the country’s policies or in writing its laws.

Qatar’s constitutional rights are shared as sparingly as in apartheid-era South Africa or Ian Smith’s Rhodesia. Only Qatari citizens — roughly one-sixth of its legal population — can purchase land or participate in government decision-making. The courts are controlled by the ruling family; the final legal appeal is to the emir, personally. Open criticism of the emir, or his family or his



OIL RICHES: Outside the Qatar Petroleum HQ in Doha (REUTERS)

13. <https://qp.com.qa/en/Pages/Home.aspx>



CATALYST: The discovery of the underwater Pars gas field — the world's largest — transformed the politics of the Middle East¹⁵

ministers, is a crime according to its constitution.¹⁴

Yet, for years, Qatar largely escaped criticism from human-rights activists, and the Western media portrayed it as a typical Gulf state: increasingly prosperous, politically quiet and aligned with the West. Both the ruling class and Western intellectuals essentially asked the same question: With all its modern infrastructure, free schooling and free medical care, why do Qatar's people need elections and government accountability?

To be sure, Qatar's neighbors have similarly poor human-rights records and lack independent courts, and its non-citizens do not enjoy the same legal rights as in Western democracies. (By contrast, Arab Israelis can buy land, vote in elections, run for office and enjoy identical legal protections to their fellow Jewish countrymen.)

Then, suddenly, an underwater discovery set Qatar apart from its equally wealthy, unfree neighbors. The 1990 discovery of the vast offshore

Pars gas field — an underwater territory larger than the land mass of Qatar itself, and the world's largest gas field — transformed Qatar and the politics of the Middle East. The sea-covered field is now divided into two major parts, the North Dome and the South Pars fields.

This discovery made Qatar much richer than any of the other Gulf states (except for its largest neighbor, Saudi Arabia), and enabled it to play a much larger role on the global stage. It did not wait long to seize its moment.

14. <https://www.theguardian.com/global/2013/jun/25/qatar-12-things-you-need-to-know>

15. Source: "Qatar 'rises above' its region: Geopolitics and the rejection of the GCC gas market," Jim Krane and Stephen Wright, Kuwait Programme on Development, Governance and Globalisation in the Gulf States, London School of Economics and Politics, March 2014, Number 35

Buying its Way as a World Influencer

Qatar soon used its vast new wealth to buy influence across the Arab world. Once hundreds of miles of undersea pipelines were completed in 1995, the petrodollars began flooding in and Qatar's regional influence rose with the tide.

The Al Jazeera media empire, owned and controlled by the Al Thani family foundation, was launched that same year. The timing is no coincidence.

The ruling family used its newfound money to broker agreements across the Muslim world, and began to fund its television channel to influence Muslim opinion, first in Arabic and then in English (the language of many of South Asia's Muslims, as well as immigrant populations in Western Europe and North America — in fact, only 313,000 [2017 figures] of Qatar's 2.69 million residents are actually citizens; the remainder are expatriates and immigrants who hail from India, Pakistan, Iran, Europe, Southeast Asia and other Arab lands).

Today, Qatar is the world's largest exporter of liquefied natural gas (a.k.a. LNG),¹⁶ making it one of the wealthiest nations on Earth on a per-capita basis (earning an \$125,000 income, the highest in the world).¹⁷ Together, Qatar's money and its *Al Jazeera* broadcasts (the name means "the peninsula" in Arabic) gave the tiny emirate enormous influence. It became, as one retired CIA official told me, the "mouse that could roar." Its leonine rumble was soon heard in nearly every conflict in the Muslim world, even disputes centered thousands of miles from its shores.

For example, as Moroccan officials in Rabat told me in 2018,



INGRATIATING: President Omar al-Bashir of Sudan (left) welcomes Sheikh Tamim bin Hamad al-Thani (center), 2014 (REUTERS)

Qatar's rulers bought a huge estate on Africa's Atlantic coast that was once owned by relatives of Morocco's King Mohammed VI.

They then gifted it back to the royal family, alleging overpayment by some \$500 million to reward other royal family members who were bickering over the money the estate would fetch. This in turn helped secure Morocco's support

To Mauritania in the south, Qatar also lavished money on imams and funded the expansion of a Muslim Brotherhood chapter.

In Sudan, Qatar's diplomats mediated the conflagration in the Darfur region, paying the major tribes not to war with each other — thus ending a genocide while buying tremendous influence with Sudan's president, Omar al-Bashir. Even as his soldiers fought Qatari proxies

in Yemen, Bashir told me in an interview in Khartoum in 2017 that he would not abandon his friends in Qatar. Meanwhile, Qatar is funding the Houthi rebels in Yemen, who are fighting its internationally recognized government.

In Syria, Qatar has funded elements of the al-Nusra Front, which is affiliated with al-Qaeda. Qatar also paid Iran-backed Syrian extremists a ransom the *New York Times*¹⁸ estimates ranges between \$770 million and \$1 billion, delivered in numerous black nylon duffel bags, for the return of 17 Al Thani family members who were kidnapped while on a week-long falcon hunt in the Iraqi desert. Such a ransom could fund a terror army for decades.

Qatar also shares its largest gas field with Iran,

16. <https://www.aljazeera.com/indepth/interactive/2017/06/qatar-north-dome-iran-south-pars-glance-lng-gas-field-170614131849685.html>

17. <https://www.nytimes.com/2018/01/22/world/middleeast/qatar-saudi-emir-boycott.html>

18. <https://www.nytimes.com/2018/03/14/magazine/how-a-ransom-for-royal-falconers-reshaped-the-middle-east.html>



POWER PLAY: above left, Nasser al-Khelaifi with former UK soccer star David Beckham in 2013 (REUTERS) and right, Khelaifi (seated) with members of the PSG soccer team at a press conference with Accor Hotels in Paris, February 2019 (REUTERS)



EYES ON THE PRIZE: Qatar's Nasser Khelaifi and Hollywood actor Leonardo DiCaprio watch the 2013 men's single semi-finals (REUTERS)

football”²⁰; London’s luxury and commercial buildings (for example, Canary Wharf Group Investment Holdings is majority-owned by Qatari Holdings — making it London’s largest property owner,²¹ according to research data firm Datscha.com); and U.S. documentary television channel *Al Jazeera America* — part of the Al Jazeera media empire — which was subsequently pulled amid claims of sexism and anti-Semitism while failing to gain sufficient U.S. audience numbers.²²

and its financial ties with the Islamic Republic are intricately interwoven.

Qatar’s banks make loans to Iran and its merchants sell Iranians a large amount of televisions, computers and other electronic goods; Iranians also factor among Qatar’s mostly expatriate populace (Qataris only comprise 11–12% of the population, with 30,000 Iranians accounting for 1.50%).¹⁹

A full accounting of Qatar’s vast diplomatic initiatives would fill pages. In short, its money and influence show up in every

conflict across North Africa, the Middle East and South Asia.

Qatar’s strategic investments include top European football (soccer) teams Málaga Club de Fútbol (CF), owned by Sheikh Abdullah ben Nasser Al Thani, and Paris Saint Germain (PSG), acquired via the Qatar Sports Initiative (QSI) headed by Qatari government minister Nasser Khelaifi — the “most powerful man in French

“

A full accounting of Qatar's vast diplomatic initiatives would fill pages — its money and influence show up in every conflict across North Africa, the Middle East and South Asia”

19. <http://priyadsouza.com/population-of-qatar-by-nationality-in-2017/>

20. <https://www.sportskeeda.com/football/top-5-football-clubs-owned-by-billionaire-arabs/5>

21. <https://www.telegraph.co.uk/business/2017/03/17/qataris-london-queen/>

22. https://www.washingtonpost.com/lifestyle/style/al-jazeera-america-news-channel-to-close-up-shop/2016/01/13/aa3ab180-ba1f-11e5-99f3-184bc379b12d_story.html?utm_term=.f60dc1d3f37a

Setting the Stage for Non-Neighborly Contention in the Region

Naturally, Qatar's sudden rise to regional leadership has provoked the ire of larger Arab states, especially that of Saudi Arabia and Egypt, whose heads tend to see themselves as the natural leaders of the Arab world.

Being the Arab world's richest nation, Saudi Arabia controls Islam's shrines in Mecca and Medina, while Egypt is home to approximately one-quarter of the world's Arab population, and its novels and televised novellas are a huge influence driving Arab culture.

Qatar's newfound wealth and its *Al Jazeera* satellite channel allowed it to compete — financially, diplomatically, militarily and culturally — with the claims to regional leadership of both Saudi Arabia and Egypt, putting it on a direct

collision course with them.

Increasingly, Qatar's diplomatic wins often seem to come at Saudi and Egyptian expense. Even Qatar's biggest prize — a U.S. military base at the Al Udeid²³ Air Base — was the result of U.S. base closure in Saudi Arabia.

Worse still, from the Saudi and Egyptian perspectives, Qatar often seemed to be working at cross-purposes with Saudi's absolute monarchy and Egypt's military dictatorship. Saudi Arabia and Egypt have generally aligned themselves with the U.S. and its diplomatic initiatives

since the start of the Iraq War in March 2003.

By contrast, Qatar has tried to simultaneously support both the U.S. and her enemies. So, while Qatar hosts a U.S. air base — home to some 11,000 American servicemen, from which U.S. warplanes strike targets in Afghanistan, Syria and Iraq — it also once housed Khalid Sheikh Mohammed, the mastermind²⁴ of the September 11 attacks, and currently shelters members of Hamas²⁵ and other terrorist groups that have killed Americans.



PRIZE ASSET: U.S. Secretary Rex Tillerson steps off the plane at Al Udeid Air Base — Qatar's biggest diplomatic asset — October 2017 (REUTERS)

23. <https://www.airforce-technology.com/news/us-qatar-support-udeid-air-base/>

24. <http://time.com/4665163/barack-obama-khalid-sheikh-mohammed-letter-september-11/>

25. <https://foreignpolicy.com/2014/08/04/hamass-bffs/>

Qatar remains one of the largest funders of the Muslim Brotherhood,²⁶ which was founded in Egypt in 1928 by Islamic scholar Hassan al-Banna, whose vision was to create a universal Islamic system of rule by promoting Islamic laws and morals through social services. This group has since spawned²⁷ virtually every radical Islamist group in the past half-century, including al-Qaeda, the Egyptian Islamic Jihad and the Islamic State of Iraq and Syria (ISIS).

Qatar fell from the high wire of official neutrality in 2017, when Saudi Arabia, Egypt, Bahrain and the United Arab Emirates announced a blockade, closing their land, sea and air ports to trade with Qatar and withdrawing their ambassadors. Qatar's Arab neighbors cited a list of reasons, including Qatar's support for international terrorism and its close relationship with Iran, which the Gulf Arab states regard as a mortal enemy.

While the U.S. and EU have tried to remain strictly neutral in the Qatar-Gulf Arab boycott, Qatar's rulers feared their neutrality would not last long. They are savvy enough to know that shifts in Western public opinion often produce shifts in government policy.



TERROR MONGER: Khalid Sheikh Mohammed, the mastermind behind the 9/11 attack (FBI/WikiCommons)

Even before the 2017 boycott began, Qatar heard prominent Americans and Europeans call for a tougher line on the gas-rich peninsula. As a result, Qatar began to compile an "enemies list."

It would not be long before it found a way to strike at its distant perceived foes, utilizing the Internet to allow it to deny all responsibility.

Fear in the Spear: Qatar's Use of Spear-Phishing

Qatar began to launch its systematic cyber warfare campaign against more than a thousand victims in North America, Europe, the Middle East and India in the past four years.

As the weakness of countermeasures has proved ineffective against these tactics, eyewitnesses have revealed how this new world of cyber warfare and diplomacy poses a risk to democracy itself.²⁸ Across its more than 1,200 cyber victims,²⁹ Qatar has used the same pattern over and over: first, it sends a spear-phishing email to an unsuspecting target. Since this looks like an ordinary email from someone in the quarry's address

book, the target will click on the email, which then launches a virus-like program that will transmit all their private emails to their attacker.

Then those emails will be catalogued by topic and recipient, and combed over for embarrassing admissions, financial irregularities or illicit relationships. As any damaging dirt is found, it is then circulated to journalists at *New York Times*, *The Washington Post*, the Associated Press and other major news outlets.

Next, as some unsuspecting, scoop-hungry and credulous journalists suddenly find this treasure trove in their email inbox, they will contact the prey for comment. Sometimes a demeaning or destructive story is subsequently published, which will quickly metastasize from one news outlet to another, instantly devouring the prey's good name. At other times, reporters are unable to verify the email contents independently, so

26. <https://www.aljazeera.com/indepth/features/2017/06/muslim-brotherhood-explained-170608091709865.html>

27. <https://www.hudson.org/research/13787-the-rise-of-the-violent-muslim-brotherhood>

28. <https://www.bloomberg.com/opinion/articles/2018-09-18/russian-hackers-aren-t-the-only-ones-to-worry-about>

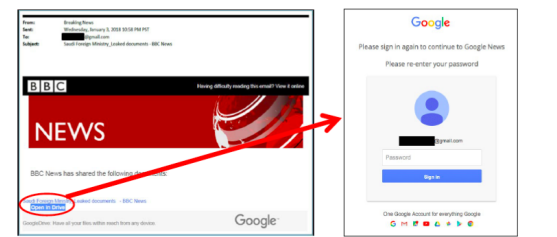
29. <https://english.alarabiya.net/en/features/2018/09/30/EXCLUSIVE-Why-the-fight-against-Qatar-s-US-cyber-attacks-is-not-over-yet.html>

no story is published. But the reporter's phone call, by itself, would send the prey an intimidating message: that it is risky and reckless to oppose Qatar.

Either by shaming or destroying Qatar's perceived enemies, such spear-phishing techniques have undermined much of the opposition to the emirate's policies inside Western democracies.

According to DigitalGuardian.com, spear-phishing is the most successful form of acquiring confidential information on the Internet, accounting for 91% of attacks.³⁰ Unfortunately, with such a dangerous precedent being set, nothing can stop Iran, North Korea or other rogue nations from adopting the same playbook. Indeed, they may already be doing so... while eluding detection by intelligence services.

SHORTENED LINKS USED IN SPEAR-PHISHING



Attackers sent spearphishing emails from email addresses designed to look legitimate, such as donotreply@bbcnews@gmail.com and noreply@servicealerts@gmail.com.

The spearphishing emails include the shortened links created by attackers.



The shortened links lead victims to fake webpages designed to look like authentic sign-in pages.

Attackers control the fake webpages, stealing victims' credentials.

After entering credentials, victims taken to webpage advertised in spearphishing email.

Representative IP Addresses Used By Attackers

Internet Service Providers

78.100.98.117 – Registered to Ooredoo (Qatar)

Virtual Private Network and Virtual Private Server Providers

31.170.164.21 – Registered to Hostinger (Cyprus)

77.73.68.252 – Registered to Fishnet Communications OOO & VEESP SIA (Russia)

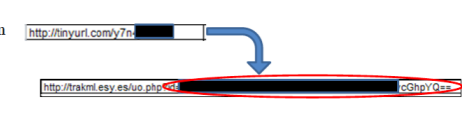
185.42.223.75 – Registered to Clouvider (United Kingdom)

185.42.223.199 – Registered to Clouvider (United Kingdom)


IP ADDRESSES: The list shows the trail of VPNs registered to Qatar

DATA SHOWS ATTACKERS' TARGETS

8,000 long links contain embedded encoded Base64 text, in which plain text appears as binary code.



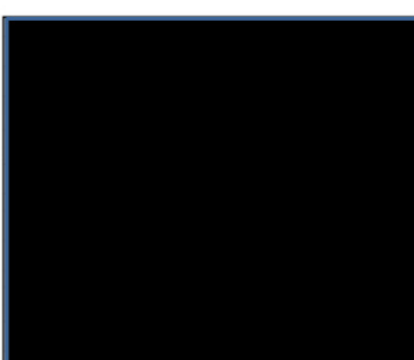
Decoding Base64 text reveals more than 1,200 unique email addresses belonging to attackers' targets.



SPEAR-PHISHING TACTICS: The charts above and below show how spear-phishing is done. Note that phishing attacks are not tailored to the victim, while spear-phishing attacks are

DECODED NOTES SHOW TARGETS TRACKED AND ATTACKED

Attackers' Code



Decryption

CSVRB	@hotmail.com.....attack.....BITA
RSQUNLSU5HLI4uLI4uLI4uLI4	@hotmail.com.....TRACKING.....BITA
uZy4uLI4uLI4uLI4uLI4uLI4uLI4	@yahoo.com.....tracking.....BITA
LI4uLI4uLI4uLI4uLI4uLI4uLI4	@yahoo.com.....tracking.....BITA
uLI4uLI4uLI4uLI4uLI4uLI4uLI4	@hotmail.com.....tracking.....bita
uLI4uLI4uLI4uLI4uLI4uLI4uLI4	@yahoo.com.....tracking.....BITA
uLI4uLI4uLI4uLI4uLI4uLI4uLI4	@hotmail.com.....attack.....bita
uLI4uLI4uLI4uLI4uLI4uLI4uLI4	@hotmail.com.....JUST_TRACKING.....BITA
uLI4uLI4uLI4uLI4uLI4uLI4uLI4	@hotmail.com.....TRACKING.....BITA
uLI4uLI4uLI4uLI4uLI4uLI4uLI4	@hotmail.com.....tracking.....bita
uLI4uLI4uLI4uLI4uLI4uLI4uLI4	@hotmail.com.....attack-2.....BITA
uLI4uLI4uLI4uLI4uLI4uLI4uLI4	@yahoo.com.....x.....BITA
uLI4uLI4uLI4uLI4uLI4uLI4uLI4	@hotmail.com.....TRACKING.....BITA
uLI4uLI4uLI4uLI4uLI4uLI4uLI4	@hotmail.com.....T-Ri
uLI4uLI4uLI4uLI4uLI4uLI4uLI4	@hotmail.com.....tracking.....BITA
uLI4uLI4uLI4uLI4uLI4uLI4uLI4	@hotmail.com.....x.....BITA

Operation code names identified – possibly individuals or agencies involved in attack:

- BITA / bita
- ester
- sophia

30. <https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing>



FOOLED: Eventually the cyber criminals were able to snare Robin Broidy (seen here with husband Elliott in 2012 during happier times) (Alex Berliner/ABImages, via Associated Press)

Qatar's Prominent Cyber Victims in North America: The Elliott Broidy Case

Elliott Broidy, a self-made successful entrepreneur and Beverly Hills-based financier, was Deputy Finance Chairman of the Republican National Committee and a close friend of President Trump.

Broidy was also known to be a very outspoken critic of Qatar, citing its human-rights record, financial support for terrorism and closeness to Iran — a theocratic state that is developing nuclear devices and the long-range rockets to carry them. Broidy's combination of political connections, personal views and indiscretions made him the perfect target for Qatar's spear-phishing efforts, he said.

Jassim al Thani, a Qatari spokesman and member of the ruling family, calls Broidy's claims "completely fabricated and without merit."³¹ In an attempt to hide their locations and the origin of the

attack, the hackers used a Virtual Private Network Service providers registered in different countries, including Russia, Cyprus, the United Arab Emirates and the U.K.

However, their plan fell apart when a glitch occurred for several minutes, revealing the central launch point and IP address (78.100.98.177), which was registered under Qatar's main internet service provider, Ooredoo — a company mostly owned by members of the Al Thani royal family.

Spear-phishing emails first appeared in the inboxes of a longtime friend of Broidy's and Broidy's wife, Robin, on Dec. 27, 2017. The emails seemed to be from legitimate sources or contacts in their respective email address books. Still, these initial attacks failed. One of the emails sent to Broidy's friend (who requested anonymity through a spokesman)

subsequently appeared to be a well-designed email from the BBC news network with the subject line "Saudi Foreign Ministry Leaked Documents."

Once the target clicked on the "OPEN DRIVE," he was directed to a Google news webpage that asked him to verify his own password. The hackers on the other side were waiting. Once the unsuspecting victim typed in his password, it is over — the cybercrime has been committed and the victim's credentials have been stolen.

The pace of phony emails accelerated between Dec. 28, 2017 and Jan. 4, 2018 in what Broidy's friend described as "almost nonstop attempts to spear-phish me, including text messages purportedly from Google tech support."

Eventually, the cyber predators became clever enough to fool Robin

31. <https://www.bloomberg.com/news/articles/2018-05-24/broidy-s-expanded-hack-allegations-fault-ex-spy-emirs-brother>

Broidy, whose e-mail servers were breached for the first time on Jan. 4, 2018. Broidy's friend fell victim shortly thereafter.

Once the emails were harvested, phony documents were distributed. The Institute for Law and Society, a sham Ukrainian think tank³², published a report on Jan. 25, 2018, accusing Broidy of engaging in business that would have put him in violation of U.S. sanctions in Russia on. (The fraud was crude. Broidy had never done business in Russia and had no government contacts there. But it hard to prove a negative, as victims soon learn.) The documents cited in the report were later found to be forged, likely by a foreign intelligence service.

Within a few days, David Corn, Washington, D.C. bureau chief at *Mother Jones*, a progressive magazine, received an email alerting him to the Institute's report and helpfully included a link to its website, ils.ooo.

Other journalists also received mysterious emails, too. On Feb. 7, 2018, Ben Wieder of McClatchy — a chain that operates 31 daily newspapers in 29 U.S. markets and boasts an average weekday circulation of nearly two million Americans³³ — published an article accusing Broidy of various misdeeds, based on purported copies of his private emails.

Then, on or about Feb. 25, 2018, PDF copies of Broidy's hacked emails begin appearing in the email inboxes of journalists in New York and Washington, D.C. Within the next few days, McClatchy's Wieder received forged Russian documents, distributed by ILS. But as soon as Wieder began working on the story, he was scooped by his competition.

The *Wall Street Journal*, posting at 10:48am EST on March 1, broke the news of Broidy's alleged Russian ties. In reality, Broidy had never

done business in Russia.

Days later, the *New York Times* ran a story based on Broidy's stolen emails on its front page on March 4, 2018. The next day, Broidy's attorneys notified Wieder and Viveca Novak, Wieder's editor at McClatchy, that the Russian documents were "provably false." No correction or retraction was offered and no change made to the initial article.

Similar letters were sent by Broidy's lawyers to the *Wall Street Journal* and *New York Times*. No response. Since these news organizations never returned to these allegations, it safe to say that they found no merit in the claims against Broidy. But the damage was done. The hackers had achieved their goals.

Al-Jazeera was not far behind. Its reporter phoned Broidy's executive assistant in his Century City, Los Angeles office on March 6, 2018, saying he was seeking comment on the hacked emails. He refused to leave his name, a call-back number or other contact information, making it impossible for Broidy to respond to the allegations. Nevertheless, the mysterious "reporter" left intimidating message: "Your reputation is about to be further maligned in international media."

The following day, *Al-Jazeera* ran a story on the forged Russian docs without including an effective denial from Broidy or pointing out that the documents were "provably false" and "complete forgeries."

Meanwhile, Associated Press reporter Tom LoBianco contacted Broidy's staff on March 14, asking for comment about the newly discovered evidence that George Nader, a onetime business associate of Broidy's, had served jail time in



SCOOPED: McClatchy journalist Ben Wieder (from his Twitter profile) received forged Russian documents from ILS, but was scooped by his competition

32. <http://ils.ooo/en>

33. https://www.sourcewatch.org/index.php/McClatchy_Newspapers

Europe for pedophilia almost two decades earlier. The allegation, which turns out to be true, was shocking to Broidy, who had no idea about his associate's criminal past.

This media technique is a classic of Soviet-era disinformation campaigns—"guilt by association"—in which an innocent victim is connected to a genuine malefactor with the idea that the innocent must somehow be guilty too. After all, he knew the guy.

The next day, a story by LoBianco and his colleague, Bradley Klapper, appeared on the Associated Press, outlining Nader's criminal record in Europe. The Associated Press reaches some two billion people across the world per day, according to its website. Its wire service is used by virtually every major newspaper, broadcast and online news outlet in the United States, Europe, Australia and Asia — therefore it was strategically vital to the cyberattack. A single biased story had suddenly appeared in countless major news outlets around the globe.

The AP attacks kept coming. On March 26, 2018, AP's LoBianco published another long story on Broidy, based on his stolen emails. Broidy maintained that some or all of the emails were actually forged. He patiently explained the evidence over and over again. Yet nothing could stop

the media feeding frenzy.

On March 29, 2018, *Newsweek* presented a story alleging a *quid pro quo* between Broidy

and Rep. Ed Royce, then-chairman of the U.S.

“This media technique is a classic of Soviet-era disinformation campaigns — ‘guilt by association’ — in which an innocent victim is connected to a genuine malefactor with the idea the innocent must be guilty too”

and Royce each denied the allegation. No real evidence was cited.

Next, *Washington Post* White House reporter Josh Dawsey phoned Broidy's staff on April 4. He

appeared to be the first journalist to receive physical print-outs of hacked emails, rather than PDFs, and indicated he was preparing a major story. *Wall Street Journal* reporter Bradley Hope then contacted Broidy on April 18,

saying he was investigating Broidy based what he received of Broidy's purloined private emails.

On April 27 AP's LoBianco informed Broidy's longtime friend that he had received a new batch of hacked e-mails, feeding another round of investigations and allegations by the press.

The next AP piece appeared on May 21, 2018.³⁵ Soon, the news stories become a torrent that Broidy found impossible to respond to. He began spending thousands of dollars per month to hire PR consultants to, as he described it, “drink from the firehose.”

It is worth noting that every reporter in this chain seems to have had a separate angle, a little “exclusive” drawn from different sections of the private emails. This meant that the victim would have to simultaneously contend with multiple bogus claims. It was fighting the hydra of ancient

Greek mythology, a multi-headed serpent which, when you cut off one head, immediately grows two more.

Even Broidy, a man with vast personal resources and longtime personal relationships with the president and other key White

House personnel, was powerless to stop the largely baseless attacks in the media. How could a lesser mortal possibly survive such an onslaught?



34. <https://www.newsweek.com/ed-royce-elliott-broidy-marie-royce-trump-administration-job-864214>

35. <https://www.apnews.com/a3521859cf8d4c199cb9a8567abd2b71>



BOLLYWOOD BASHING: Bollywood actor Anupam Kher (left) and Indian director Mahesh Bhatt (right) were among 52 Indian celebs who were also targeted (REUTERS)

Other Prominent Hacking Victims' Stories

Broidy's story is similar to that of many other hacking victims. But while Broidy's proximity to President Trump made him a lightning rod for the hackers, some received only a few negative mentions in the press.

And while this appears to be largely a result of their relative obscurity, it does not take away from the impact of the hacking on the victims' personal lives and freedom — clearly, even relative obscurity cannot serve as an effective shield against cyberattacks.

Consider the case of eight U.S.-based Syrian dissidents and other vocal Arab-Americans — Jihad Makdissi, former Syrian Foreign Ministry spokesman; Syria Emergency Task Force Managing Director Mouaz Moustafa; Saudi American Public

Relations Affairs Committee Founder and President Salman Al-Ansari; The Syria Campaign ("Americans for a Free Syria") advocacy manager Kenan Rahmani; Syrian Center for Media and Freedom of Expression executive director and The Syrian Observer editor-in-chief Wael Sawah; Lebanese-born, Washington, D.C.-based political activist Khaled Saffuri, noted for his comments on the Jamal Khashoggi case; People Demand Change Inc. executive director and former Syrian Emergency Task Force

director Sasha Ghosh Simonoff; and People Demand Change co-founder and former Syrian diplomat Bassam Barabandi — all of whom have been outspoken in their opposition to Syria's Assad government (which is backed by Iran and Qatar). They, too, were targeted and maligned in the media, as reported in the *Daily Beast*.³⁶

Rahmani's LinkedIn profile was mocked and alleged to contain several bogus claims on a website³⁷ claiming to be the "The Real Syrian Free Press," which alleged Rahmani didn't really attend law

³⁶ <https://www.thedailybeast.com/why-did-qatar-try-to-hack-syrian-opposition-leader>

³⁷ <https://syrianfreepress.wordpress.com>



SYRIAN CRISIS: Kenan Rahmani (from his LinkedIn profile) was one of several U.S.-based Syrian dissidents who were also targeted and maligned in the press

school in Washington, D.C. as he is “never there.” Sawah³⁸ admitted surprise at Qatari attempts to hack his account, affirming that Doha assaults anyone against its ally, the al-Nusra Front.

Siminoff believes he and Barabandi were targeted because of their communication with the Turkish government over the Syrian opposition, specifically trying to comprehend Qatar’s involvement, including its connections to Jabhat al-Nusra and HTS in Syria (as an independent analyst who prefers to remain anonymous explained, “Every time we follow a deal between Iran and pro-Iran militias and Islamic extremists in Syria, we find Qatari money”).

In a strange twist of irony, Siminoff says that while he formerly helped train Syrians to avoid cyber traps laid by the [Assad] regime or the Iranians, “I never thought we’d also have to

worry about the Qataris.”

Former Cairo-based *Al Jazeera English* bureau chief Mohamed Fahmy, an award-winning Canadian-Egyptian investigative reporter who was jailed in Egypt in 2014 on alleged terrorism charges and sentenced to seven years’ imprisonment, had a falling out with the Qatari-owned media network and subsequently sued his employer.

While behind bars during the 438 days of his incarceration, Fahmy overheard eye-opening confessions from members of the Muslim Brotherhood, who told him endless stories of their cooperation with the Qatari-owned *Al Jazeera* network. Fahmy has since decried this unethical and illegal relationship as being far from the fundamentals of journalism that landed him in prison.

The Qataris launched an extremely well-organized plan to steal Fahmy’s emails, assassinate his character and discredit him in a cyber-espionage operation, which Fahmy reported to the Canadian police in 2016.

Fahmy explained, “I deleted many of the spear-phishing emails I received that were clearly very well tailored to my interests as a journalist and human rights advocate, but I must have unknowingly fallen for one of them.

“I found out about it when journalist David Kirkpatrick from

the *New York Times* contacted me in 2016 to inform me he had received a flash drive from an anonymous source including copies of my stolen emails.

“Once some of the content of my emails surfaced in the story he wrote, the next day *Al Jazeera* went all out with back-to-back coverage about some of the content of the emails. Interestingly, *Al Jazeera* disclosed information that was on the flash drive but had not been included in the article published in the *New York Times*.

“I learned later from my own investigations that this is a trend the Qatari intelligence uses to distance themselves from the cybercrime by handing the goods to other news

“

I learned later from my own investigations that this is a trend the Qatari intelligence uses to distance themselves from the cybercrime by handing the goods to other news outlets and sourcing it to them when reporting the news on Al Jazeera”

—Mohamed Fahmy

outlets and sourcing it to them when reporting the news on *Al Jazeera* — their most cherished foreign policy tool and the dagger they use against the critics of Qatar.”

38. <https://qatarileaks.com/ar>



STARSTRUCK: Qatar recently acquired leading independent film producer Miramax Films, seen here receiving a 2008 “Best Picture” Oscar for “No Country for Old Men” (REUTERS)

Another prominent hacking target was Mr. Ronald Sandee, a former analyst in the Dutch military intelligence who now serves as co-founder of Amsterdam-based advisory and consultancy firm Blue Water Intelligence.³⁹

As Sandee explained in an interview with *TIJ*, “It is clear the hack targeted Qatar’s enemies and friends alike. Qatar targeted its own clients in Syria, the Muslim Brotherhood, to keep control of their activities. But targeting U.S. citizens on U.S. soil should not be without repercussions.

“This massive hacking operation, which might still be ongoing, can only be done by governments.” Sandee confirmed he continues to research the hack.

As Sandee pointed out, even Bollywood (including its Tamil Nadu equivalent, known as Kollywood, and the Telugu variant, Tollywood), was not immune to Qatar’s cyber wrath. Some 52 Bollywood actors, actresses, directors, film executives and other cinema personnel were targeted by Qatar’s hackers, as confirmed by a list in *The American Spectator*.⁴⁰

This list featured prominent Tamil actor Arun Vijay, Tollywood actors Mahesh Babu and Manjima Mohan, and Trisha Krishnan, all of whom reported hacks of their personal social media accounts.

Added to the 48 other Bollywood actors identified on the list, Qatar is suspected of hacking — or being in league with Turkey-based cyber groups ProPak and Ayyildiz Tim to hack — the accounts of actors Abhishek Bachchan, Karan Johar, Rishi Kapoor, Rakul Preet, Sruti Haasan, Ali Zafar, Boney Kapoor, Anupam Kher, Amitabh Bachchan, Arshad Warsi, Hansika and Shadi Kapoor, and Indian director Mahesh Bhatt.

It is not clear exactly why Qatar would wish to hack these Indian celebs as, unlike its other targets, none have been particularly noted for speaking out against the emirate or publicly

querying its political activities.

However, as Qatar has strategically invested in some 38 media and sports channels in geographically diverse

locations across Europe, Asia and North America — including its 2016 purchase of Hollywood’s Miramax Films — the hacks could

be symptomatic of the emirate’s ambitions to rule the global media sphere.

With 43% of the film box-office revenues made in India, Bollywood’s substantial earnings and influence would easily place it on Qatar’s hit list of rivals. As there is also a sizeable Indian immigrant population — approximately 650,000 — living and working in Qatar, the hacks could be part of a larger plan to wield influence on the subcontinent and abroad.

“
**This massive
hacking operation,
which might still be
ongoing, can only be
done by governments”**
—Ronald Sandee, *Blue
Water Intelligence*

39 <https://blue-water-intelligence.com>

40. <https://spectator.org/exclusive-the-india-files-dozens-of-bollywood-and-tollywood-actors-targeted-and-hacked-by-qatar/#.XGcmEFzuhXs.twitter>

A Not-So-Sporting Player

In addition to the Bollywood hacking assault, eight Egyptian soccer players were also targeted: Abdallah Said, Ahmed Saed, Ahmed Salama, Ayman Refaat, Islam Saleh, Mahmoud Hamdi al-Wensh, Mohamed Abdel Fattah, and Egypt and Al Ahli goalkeeper Mohamed Al Shenawy, each of whom had their private email correspondences stolen.

As per its Bollywood victims, there does not at first glance appear to be any motive for Qatar in targeting these individuals, apart from its strategic power-playing in the sports arena, both regionally and abroad.

As Sandee commented: “The targeting of a group of young football⁴¹ players by this Qatari hacking operation is disturbing. What are the Qataris looking for? Do they try to find dirt so they can blackmail these players when are participating in 2022 World Cup Football? Do they try to find weaknesses so they have leverage when they try these players out for Paris Saint Germain? Or is there even a darker agenda behind these specific hacking targets?”

The “darker agenda” Sandee alluded to shows up in another of the emirate’s sports connections. Qatar has not only established itself as a major player in European soccer through its purchase of PSG and Málaga CF, but also through its BeIn Sports media channels — formerly known as *Al Jazeera Sports* — which includes local variants such as *BeIN Sports France* and *BeIN Sports Spain*.

After the Doha-based network obtained exclusive rights to broadcast major football leagues such as the



STUNG: Egypt and Al Ahli goalkeeper Mohamed Al Shenawy, seen here during the 2018 FIFA World Cup, was one of eight Egyptian soccer players targeted by a Qatar-led email hack (Кирилл Венедиктов / WikiCommons)

41. <https://dailycaller.com/2019/02/11/qatar-hacks-egyptian-soccer-players/>

“

The targeting of a group of young football players is disturbing. What are the Qataris looking for? Do they try to find dirt so they can blackmail these players when they are participating in the 2022 World Cup Football? Or is there an even darker agenda behind these specific hacking targets?”

— Ronald Sandee



FIFA World Cup, the UEFA Europa League and the English Premier League, its Arab power rival, Saudi Arabia, disappointed sports fans by blocking the channel from broadcasting the 2018 World Cup, threatening a 10,000 riyal (\$2,746) fine to any hotel that refused to censor the network.⁴²

The Saudi-initiated Doha blockade was followed by other Gulf states⁴³ (the UAE, Egypt and Bahrain, among others), escalating in a diplomatic row over Qatar's financial backing of media channels and its support for Iran and the Muslim Brotherhood.

The Gulf blockade was also publicly backed by Trump, who accused Qatar of supporting terrorism and cited Elliott Broidy as a key influence in his policy. As Qatar was subsequently hit with international sanctions, it appears the emirate may have specifically

targeted Broidy as an act of retaliation because of his influence on Trump.

Speculating on the rationale for the attack on the soccer players, David Reaboi, senior vice president at the Security Studies Group⁴⁴ in Washington, D.C., said: “These actions are fully in line with Qatar's subversive policy, in addition to the billions spent by Qatar in organizing the World Cup, and their clear willingness to do all the suspicious things to ensure access to the organization and to use football as an instrument of influence.

“There are many reasons for Qatar to penetrate the means of communication for known people, including silencing critics, and in this case, maybe to influence the Egyptian players to sabotage the Egyptian team.”

As in Qatar's other cyber warfare strategies, “sabotage” is clearly the name of the game.

“

There are many reasons for Qatar to penetrate the means of communication for known people, including silencing critics; in this case, maybe to influence the Egyptian players to sabotage the Egyptian team”

— David Reaboi, Institute for Security Studies



42. <https://www.alaraby.co.uk/english/news/2017/6/13/saudi-arabia-blocks-qatari-owned-bein-sports-channel>

43. <https://www.bbc.co.uk/news/world-middle-east-40246734>

44. <https://securitystudies.org>

Ambassador Lee Wolosky Cracks the Hackers' Code

Broidy's story is similar to that of many other hacking victims. But while Broidy's proximity to President Trump made him a lightning rod for the hackers, some received only a few negative mentions in the press.

As soon as Elliott Broidy realized he was being cyberattacked, he spared no time in fighting back, quickly hiring prominent Boies Schiller Flexner, LLP lawyer and former U.S. Special Envoy to Guantánamo Lee Wolosky, who filed a lawsuit in California in March 2018 against Qatar and their agents in the U.S.

Of the unique lawsuit, which attempted to hold a foreign government accountable in a U.S. court for digital espionage operations,⁴⁵ Wolosky said that hacking into a U.S. citizen's emails is a criminal offense, but it is tantamount to "an act of war when such an attack is orchestrated by a foreign government."

Wolosky is a seasoned litigator, crisis manager and counterterrorism official who has served under the three past



HACK CRACKER: Broidy hired Boies Schiller Flexner, LLP lawyer and former U.S. Special Envoy to Guantánamo Lee Wolosky to represent him in his suit against Qatar

U.S. presidents in significant national security positions. In 2016 he was accorded the personal rank of Ambassador by then-President Obama, who called on Wolosky to lead U.S. diplomatic efforts to close the U.S. detention facility in Guantánamo Bay, Cuba.

Wolosky explained to *TIJ* in an interview how this lawsuit unraveled the data about the hundreds of people targeted and who is behind it:

"The IP addresses came off the Broidy's capital management server, which, like many servers, logs off all of the internet protocol addresses that seek access to the server.

"And what that revealed was a very sophisticated computer-hacking operation that used VPNs all over the world to try and disguise the origin of the

computer attacks.

"What this means, in simple terms, is that the attackers bounced their internet traffic of computer servers all over the world. Really, in most continents, we found thousands of computer servers even just within the United States that were used to try and disguise their activities.

"However, in a couple of instances, their obfuscation techniques failed. The VPNs failed, and our technical people were able to see through — directly to the originating internet protocol address.

"It was sort of like someone operating behind the curtain and then the curtain falls down, and you're able to see who's behind the curtain. And in those cases, we saw the use of a single internet protocol address in Doha, Qatar, as standing behind the curtain."



The attackers bounced their internet traffic of computer servers all over the world. In most continents we found thousands of computer servers that were used to try to disguise their activities"

— Ambassador Lee Wolosky

45. <https://www.politico.com/story/2018/05/24/elliott-broidy-qatar-email-hack-607970>

US-based company Tiny Url, a shortening web service that provides short aliases for redirection of long URLs, was among the companies that had to comply with the court's order and cooperate with the investigation.

Essentially, the investigation into how the hackers used thousands of "Tiny Urls" led to the revelation that this crime was not only directed against Broidy, but also towards the thousands to whom the corrupt links were sent.

Wolosky, in his legal battle on behalf of Broidy, succeeded in convincing the court to issue 80

subpoenas in his quest to pinpoint the cyber thieves: "We were able to get all of the data used by this group over a one-year period from May 2017 to June 2018 through the U.S. legal practice of subpoena.

"When we got that data and decoded it, we were able to see all the fake emails and all the fake addresses that were used by the group in targeting particular email accounts — real email accounts.

"As a result of obtaining the email accounts and the fake emails, we were able to see exactly who was targeted by their email address, and when they were targeted — we even

saw some notes that were indicated next to their targets, and these were the notes of the attackers saying what they wanted to do.

"In some cases, the hackers created fake emails based on the general narrative of the real emails, so you're talking about an operation that involved probably thousands of people, certainly hundreds of people in order to do all this work.

"And it's really only states, in our experience, that have the resources to run an operation of this size and this magnitude and sophistication."



Masterminds of the Hack Named in Broidy's Lawsuit

During the lawsuit, Broidy asserted that the hack's ring leader was former high-ranking UN diplomat Jamal Benomar, whom he accused of serving as an undeclared agent of Qatar⁴⁶

Born in Morocco (but a dual Morocco-UK citizen), Benomar was a student opposition leader who was briefly jailed in the 1970s and

1980s, nevertheless managing to obtain a Bachelor's and two Master's degrees from the Sorbonne while imprisoned.

Eventually, after managing

to escape Morocco through the interventions of Amnesty International, he charmed his way into the UN's diplomatic corps. By 2009, the native Arabic speaker

46. <https://www.politico.com/story/2018/07/20/elliott-broidy-jamal-benomar-qatar-734951>



DOUBLEAGENT: Nick Muzin, a one-time Deputy Chief of Staff to failed presidential aspirant Ted Cruz, registered with the U.S. as a foreign agent of Qatar

was named UN Special Envoy to Yemen, a war-torn nation on the Southeastern edge of the Arabian Peninsula. Sent to mediate between the embattled regime in Sana'a (supported by Saudi Arabia and the UAE) and the rebels (backed by Iran, Qatar and al-Qaeda), Benomar soon befriended the Qataris.

In 2013, Benomar met with the Emir of Qatar. Soon after, Qatar gave \$350 million to the Yemen Compensation Fund following the meeting.⁴⁷ How this money was spent is of great controversy. Political analyst Ahmed Sinan⁴⁸ has accused Qatar of funding the Yemeni off-shoot of the Egyptian Muslim Brotherhood, which has historically been at odds with Saudi Arabia.

Said Sinan, "The sizable donation from the Qataris is a way to decrease Saudi influence in Yemen. Benomar became an agent working on behalf of Qatar."

By some accounts, Benomar accepted bribes from the Qataris equal to \$2 million per month. After the illicit arrangement became public in 2014, Benomar was relieved of his UN post for reasons that were not made public (officially, he resigned in April 2015, and was

reappointed as UN Special Adviser at the level of Under Secretary-General in November 2015).

Soon, Benomar found work directing a cyber-warfare consulting firm in London, according to Broidy's court filings, which suspected Benomar of developing the

global target list of Qatar's enemies.

Allegedly working under Benomar was an unlikely collection of failed but ambitious political manipulators, including Jewish Americans Nick Muzin, former Deputy Chief of Staff to U.S. Senator and presidential aspirant Ted Cruz, and Joseph (Joey) Allaham, the one-time "King of kosher" restaurants in New York.

Both Muzin and Allaham registered with the U.S. government as paid foreign agents of Qatar, with Muzin alone receiving \$300,000 per month, according to *Mother Jones*.⁴⁹

(After receipt of Wolosky's subpoenas, Muzin and Allaham ended their work for Qatar, with an embittered-sounding Allaham subsequently telling *Politico* that "Qatar enjoys portraying themselves as purveyors of peace in the

region, but nothing could be further from the truth.")

The civil case filed by Elliot Broidy was eventually dismissed. Benomar, who left the U.N. before the alleged hack, submitted documents stating that he is a Moroccan diplomat, posted to the North African nation's mission to the U.N.

The U.S. recognized Benomar's diplomatic immunity despite the fact he is a permanent resident⁵⁰ of the U.S., which would normally bar him from a diplomatic immunity claim. Benomar has owned property in Georgia and New York and his wife and children legally reside in the U.S.

Equally mystifying is that Benomar was also named as a Member of the Supervisory Board of Lagardère SCA, a multinational media conglomerate with travel and sports and entertainment subsidiaries headquartered in Paris, in September 2018. Lagardère is a publicly traded company and Qatar is Lagardère's top investor.⁵¹

However, the fact Benomar is working for a publicly traded company undermines his claim to be working as diplomat for Morocco.



MYSTERY: Benomar joined the Supervisory Board of Lagardère SCA, a Paris-based multinational media conglomerate whose top investor is Qatar, in September 2018 (REUTERS)

47. <https://www.arabianbusiness.com/qatar-pledges-350m-yemen-fund-for-sacked-civil-war-workers-517633.html>

48. <http://hlnr.org/arabic/activitydetails.php?id=02xnZg==#.XIF91YVzy1s>

49. <https://www.motherjones.com/politics/2018/06/joey-allaham-nick-muzin-qatar-jewish-leaders/>

50. <https://staging.washingtontimes.com/news/2018/nov/15/jamal-benomar-defendant-in-hacking-case-shielded-b/>

51. <https://www.reuters.com/article/lagardere-qatar-idUSL8N1I55NJ>

Trump's Cyber-Terrorism Strategy is Not Enough

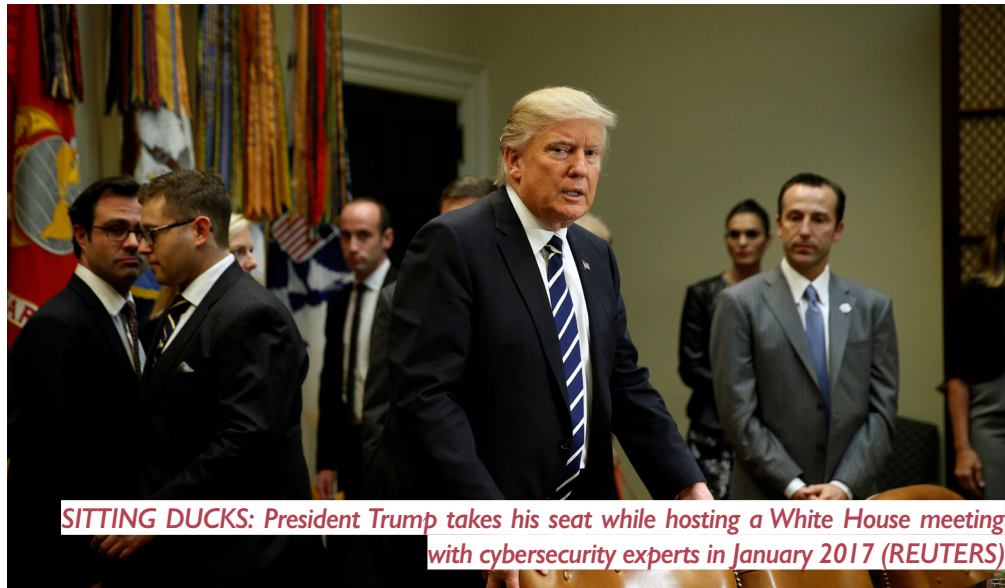
While President Trump recently unveiled a new cybersecurity strategy⁵² building on his Executive Order “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” signed in May 2017, it leaves out an important component: victims of hacking, such as Broidy and the 1,400+ others.

But effective countermeasures to national hacking attacks are hard to come by.

Military actions are essentially off the table, as no nation has yet carried out military strikes based cyberattacks. While sinking ships, hijacking planes or kidnapping citizens has provoked military strikes in U.S. history, non-physical raids have never drawn a military response. It is hard to imagine any elected leader ordering air strikes following a cyberattack.

But what about cyberattacks in response to cyberattacks? While it has a nice parallelism, the U.S. Cyber Command has not announced such a policy, and there is no public evidence that the U.S. has ever used to hackers to strike back at foreign hackers. A recent *Wall Street Journal* op-ed⁵³ called for “a cyber second-strike capability” but, for now, that remains a matter of advocacy, not policy.

While sanctions are often proposed to counter digital attacks, they are very rarely, if ever, imposed. Diplomats want hard evidence that a particular nation's



SITTING DUCKS: President Trump takes his seat while hosting a White House meeting with cybersecurity experts in January 2017 (REUTERS)

government ordered or condoned the attacks. This kind of evidence is very hard to obtain since rogue nations typically use third-party clandestine operatives (such as Indian or Ukrainian hackers) who use offshore proxy servers located in the Philippines or Malaysia to launch such attacks. Nor do governments ever publicly announce their culpability — and, indeed, they usually deny any responsibility or knowledge of those attacks.

Criminal charges against state actors are also difficult, since prosecutors must show “guilt beyond a reasonable doubt.” That evidence is rarely available, and no foreign citizen residing outside

the U.S. has ever been successfully prosecuted in American courts. What's more, U.S. law gives foreigners immunity from U.S. prosecution, if the alleged crimes were committed outside the United States. Very few victims try to bring lawsuits against foreign malefactors in U.S. courts.

Broidy's first lawsuit in a Los Angeles federal court was dismissed in the spring of 2018. The judge cited the 1976 Foreign Sovereign Immunities Act, which safeguards⁵⁴ non-U.S. citizens such as Benomar from facing lawsuits in U.S. courts.

The judge went so far as to beg, in writing, for Congress to amend the law to cover cyberattacks as it did in 2016 to permit foreign terrorists to be sued in U.S. courts, but his suit was unsuccessful.⁵⁵



HACK VICTIM: Bahrain's Crown Prince Salman bin Hamad al-Khalifa (REUTERS)

52. <https://www.whitehouse.gov/briefings-statements/statement-president-regarding-national-cyber-strategy/>

53. https://www.wsj.com/articles/strike-back-against-every-cyberattack-11548624081?shareToken=stcb9063d387dc48e786f564b94cd73703&ref=article_email_share

54. <https://www.reuters.com/article/us-usa-trump-russia-broidy/trump-fundraiser-broidy-hit-with-another-setback-in-qatar-lawsuit-idUSKCN1OK2EA>

55. <https://www.nbcnews.com/politics/national-security/u-s-says-defendant-elliott-broidy-hacking-case-has-diplomatic-n935456>

QATAR'S CYBER TARGETS: (main image) Secretary-General of the Arab League and former Egyptian foreign minister Ahmed Abdul Gheit (REUTERS); (Insets, from their Twitter accounts): Assistant Secretary-General of the Arab League and former Egyptian ambassador Hossam Zaki; and UAE official and diplomat Sheikh Maktoum Bin Bhutti al Maktoum;



Cyber Diplomacy and Its Risk to Democracy

Check HaveIBeenPwned.com and see if you have been hacked.

It is highly likely your secret passwords and bank details are already for sale on the “dark web.” More than 700 million accounts are already compromised, according to *The Wall Street Journal*.⁵⁶

In theory, democracies flourish when competing factions air their best arguments and majorities form a new consensus based on evidence and argument. In reality, some ideas are hampered by lack of financial support, and are therefore kept from public consideration. Others lack charismatic champions to present contrary

ideas in the best possible light.

But each of these democratic flaws still contains an element of democracy itself: funders vote by donating money to movements (or not), and powerful personalities agree or disagree to champion unpopular ideas. Cyber warfare represents a new and unprecedented attack on democracy itself.

By silencing dissenting voices, Qatar — or any other rogue nations — can divert or distort the national conversation by keeping facts or ideas from the public. Like a jury denied exculpatory evidence, voters may render their verdicts on incomplete or even false information.

Imagine if Russian President Vladimir Putin’s jailing of journalists or killing of dissidents was kept from the public. Without this knowledge, voters may come to a very different conclusion about the wisdom of sanctions against Russia.

Likewise, imagine if China’s unprecedented

“
If every critic had to face the possibility that his advocacy would be undermined by publicizing his private shortcomings, only saints or fools would challenge dictators. This would leave a world in which many leaders are afraid to ‘speak truth to power’ — and we will all be poorer as a result”
”


56. https://www.wsj.com/articles/strike-back-against-every-cyberattack-11548624081?shareToken=stcb9063d387dc48e786f564b94cd73703&ref=article_email_share

build-up of its naval forces were kept out of the newspapers. Voters may come to a different conclusion about the wisdom of enlarging America's navy. Or, imagine if Syrian dictator Bashar al-Assad's use of poison gas against women and children was never brought to the West's attention, or the genocide in Sudan's Darfur region were never made known... the list goes on.

If every critic had to face the possibility that his advocacy would be undermined by publicizing his private shortcomings, only saints or fools would challenge dictators. This would leave a world in which many leaders are afraid to "speak truth to power" — and we will all be poorer as a result. It will also be a world in which autocratic rulers can

terrorize not only their own people, but even the free peoples of Western democracies.

This changes the power dynamics, the *realpolitik*, of the globe by making politicians, journalists, missionaries, dissidents and others, slavishly fearful. It is the cyber equivalent of giving dictators a nuclear bomb. And no arms control treaty can disarm them.

If Western democracies do not develop effective countermeasures to what former U.S. president Bill Clinton once called "the politics of personal destruction," the leadership of the world will slip into the hands of the most ruthless — a scenario where whoever is willing to be the most personally destructive will rule the rest. 



Richard Minter

Richard Minter is an award-winning investigative journalist and author whose articles have appeared in the *New York Times*, *The Washington Post*, *The Washington Times*, *The Wall Street Journal*, *The Atlantic Monthly*, *Newsweek*, *The New Republic*, *National Review* and *Reader's Digest*. He is the author of three *New York Times*-bestselling books, *Losing Bin Laden*, *Shadow War* and *Leading From Behind*. Formerly an editorial writer for *The Wall Street Journal* in Brussels and a member of the *Sunday Times*' investigative reporting team in London, Minter currently serves as a national security adviser for *Forbes* and CEO of the American Media Institute. CSPAN's Brian Lamb cited Minter's investigative work on 9/11 mastermind Khalid Shaikh Mohammed as one of his top book author interviews of the past 25 years. He resides in Washington, D.C.

View more of our reports at:

www.investigativejournal.com/reports



