Gulf split heralds new uses for cyber capabilities

Tuesday, February 6, 2018

Regional tensions among Gulf Arab countries highlight the increasing salience of the online world


A staff member at Qatar News Agency in Doha (Reuters/Tom Finn)

Gulf social media are today involved in a battle of hashtags over an alleged Qatari call to 'internationalise' the holy sites in Saudi Arabia's Mecca and Medina -- a call Doha says it never made. The Qatar crisis in June 2017 was similarly sparked by a piece of 'fake news' planted on Doha's national news agency showing the Qatari emir as expressing support for Iran and the Muslim Brotherhood movement. The incidents are part of a rising trend of offensive cyber actions and government-backed social media contestation in the region. They may also be the first examples of a combined cyber and physical strategy achieving core foreign policy goals just short of actual conflict.

What next

Some Gulf Cooperation Council (GCC) countries will increasingly use cyber operations to achieve geopolitical ends, as do other highly connected states. However, like their main ally Washington and their major adversary Tehran, they will seek to keep such actions from triggering actual conflict by maintaining ambiguity of attribution. Contractors will generally be used for these operations, due to their deniability and relatively low costs, but their use could create political and reputation risks through leaks and conflicts of interests.

Subsidiary Impacts

- The GCC's high online presence and draconian regulatory framework will make social media a key arena for covert state action.
- Interpretation of past events will fragment, meaning divisions such as the GCC split harden over time and become difficult to reverse.
- As GCC states' attitudes to Iran diverge further, their Western allies will find regional diplomacy more labour-intensive.

Analysis

Saudi Arabia, the United Arab Emirates (UAE), Egypt and Bahrain ('the quartet') on June 5, 2017 launched a political and economic boycott of Qatar: recalling citizens, withdrawing ambassadors and cutting land, air and sea links (see QATAR: Arab enemies may impose new sanctions - June 26, 2017).

The boycott was the culmination of a long cycle of dispute and reconciliation between Qatar and its neighbours. Its general justification was Qatar's support for 'terrorism', defined broadly to include backing for opposition groups elsewhere in the region, such as the Muslim Brotherhood, through such tools as Doha's Al Jazeera television channel (see QATAR: Doha will deploy Al Jazeera as a vital weapon - October 23, 2017). However, closer triggers included:

- the increasingly close alignment between activist Saudi Crown Prince Mohammed bin Salman and the crown prince of Abu Dhabi, Mohammed bin Zayed, who has long opposed Qatar's links with the Muslim Brotherhood; and
- the apparent backing, in his visit to Riyadh in May, of US President Donald Trump, who tweeted his support for the quartet the day after the boycott -- although this was later contradicted by the neutral stance of other US government departments and replaced by an offer of mediation.

Cyber instigation

The immediate pretext for the quartet's actions was footage of the Qatari emir that appeared on the website of Qatar News Agency (QNA) just after midnight on May 24, 2017, with text that portrayed him as expressing support for Iran and the Muslim Brotherhood.

Following its publication, news agencies in the quartet countries picked up the story almost immediately, resulting in claims that they were prepared for or tipped off about its release. At least three dailies in Saudi Arabia and one in UAE led with it in their morning headlines on May 24.

> Anonymous sources blamed Qatar's Gulf rivals

Qatar's investigation, which was supported by the FBI and the UK National Crime Agency, concluded that the appearance of the video was the result of a hostile cyber operation against QNA. Sources told the international press that the UAE or Saudi Arabia hired Russian contractors to conduct the operation.

The Washington Post reported unnamed US national security officials as saying that the intrusion was carried out by contractors working for Abu Dhabi. Separately, The New York Times cited anonymous US and Qatari officials as blaming Russian hackers for hire, and the Guardian reported observers' suggestions that the UAE or Saudi Arabia had commissioned the hackers.

In addition, the Qatari attorney-general on June 20 claimed Doha had evidence that iPhones from the quartet countries were used in the operation. Nevertheless, the attribution of cyber operations is extremely difficult, and the forensic analysis is not publicly available (see INTERNATIONAL: Impunity

will incentivise cyberattacks - December 16, 2016).

GCC cyber warfare

The QNA cyber operation follows a wider pattern of cyber tools deployed to achieve largely domestic policy and security objectives in Egypt and the GCC states. All these countries, including Qatar, have invested heavily in technologies for large-scale and targeted surveillance manufactured by companies in the United States, Europe and -- in the case of the UAE -- Israel.

> Surveillance against activists can be a bridge to offensive operations

Possession of surveillance technologies (which is mostly outsourced) has usually been revealed after their use against dissidents and activists. However, these technologies are also linked to offensive cyber activity, involving the active penetration of an adversary's networks (which would likely be carried out by the GCC and Egyptian governments themselves).

Governments in the region benefit from buying offensive cyber technologies not only through deploying the technologies themselves, but also by learning and replicating them. In addition, they develop close working relationships with cyber contractors.

Other cyber tools were also used during the Qatar crisis. The site 'Qatarileaks' was created at around the same time, carrying anti-Qatar propaganda.

Just before the ostracisation, but after the QNA incident, an unknown individual offered the private emails of the influential UAE ambassador to Washington, Yusuf al-Otaiba, to several US news outlets. These emails indicated that Otaiba had significant influence with several think tanks and government figures including Jared Kushner, as well as a lavish lifestyle and anti-Qatar posture. Their publication was probably a Qatari response to the earlier cyber operation.

Social media aspects

Both sides also recognised the importance of social media in shaping public opinion in their favour. Immediately after the boycott, the UAE attorney-general defined showing sympathy for Qatar online as a cybercrime, resulting in prison sentences between 3-15 years.

This announcement highlights the fact that all the GCC countries have broad definitions of 'cybercrime' and harsh punishments for online speech relative to international norms (see UNITED ARAB EMIRATES: Government will monitor internet - December 15, 2016).

This social media antagonism has continued. Throughout August, a popular Saudi figure on Twitter misleadingly interpreted the quantity of anti-Qatar hashtags as demonstrating popular support against the ruling Al Thani family in Qatar, even though most of those accounts were located in Saudi Arabia. In December, the popular 'Saudi citizen' account was hijacked, tweeting pro-Al Thani comments.

New strategic model?

However, unlike the QNA operation, these actions were not accompanied by a wider political strategy. Uniquely, the fake video was part of a coordinated strategy involving media coverage and immediate policy 'reaction'.

Despite Qatar's immediate denials and later evidence of tampering, this strategy was successful in isolating Qatar. Key factors included control of the press and social media, and the tactic of doubling-down on the accusations -- for example, by releasing a list of demands.

This new form of cyber action is more tightly directed than Russian disinformation campaigns against European elections, and more clearly part of a foreign policy strategy than the Russian cyber operations against Estonia were a decade ago. It is also more overt than the 'effects' operations

undertaken by US and UK intelligence agencies (which, for example, set up false online identities and resources).

Although the United States has used joint cyber-physical operations successfully against Islamic State in Syria, such joint operations are rare outside war contexts. This is therefore the first example of a combined cyber and physical strategy achieving core foreign policy goals just short of actual conflict. It may be used more frequently in future disputes.