The current crisis in the Persian Gulf in the context of hybrid warfare

Associate Professor Sascha-Dominik Bachmann, Bournemouth University and Swedish Defence University

Introduction

The Middle East, or New Middle East as it also has become known after the Arab Spring of 2011, is going through seminal geographical and political changes and challenges.[1] In the end, the Arab Spring did not lead to the advent of an Arab renaissance of democracy and good governance but only to increased regional instability. The latter has been highlighted by the rise of Islamic State (IS), firstly in Syria and Iraq, and then Libya, where it managed to exploit the vacuum left after Qaddafi.

The present crisis among the members of the Cooperation Council for the Arab States of the Gulf (GCC but known colloquially as the Gulf Cooperation Council) began when Saudi Arabia and the United Arab Emirates (UAE) cut diplomatic ties with Qatar and imposed a land, sea and air embargo in early June 2017, in response to the alleged role of Qatar in aiding and abetting Islamist terrorism in the region, as well as its diplomatic ties to Iran.

The crisis has laid bare the region's insecurities and vulnerabilities, against the backdrop of new threats to the region's stability, notably the emergence of so-called hybrid threats and hybrid warfare. This has repercussions far beyond the region for economic, strategic and religious reasons. The arrival of new strategic competitors to US interests in the region, including China and Russia, and the return of Turkey as the successor of the former colonial occupier of Arab lands, the Ottoman Empire, have complicated the situation.

This short contribution discusses the present crisis within the context of security and conflict-related observations from the region, being played out through hybrid warfare, concluding with a brief synopsis of Qatar's potential countermeasures.

The GCC as a focal point of Gulf prosperity and the need for regional security

The GCC states represent some of the wealthiest states in the world (in terms of GDP per capita). After the discovery of oil in many Gulf nations, they united as the world's main oil producers: Saudi Arabia alone is the second-largest producer of crude oil after Russia, and the GCC's share of global oil reserves accounts for about 70 per cent of all global reserves.[2] The global dependency on oil (and liquefied gas) is set to continue, despite increasing initiatives among the G7 states to find non-fossil fuel alternatives, compounded by the steady industrialisation and urbanisation of countries such as India and China.

Consequently, the security and stability of GCC countries has become a matter of global concern. Western nations, in particular, due to their political, military and security interests, have sought to strengthen security in the region, with the US-GCC Strategic Cooperation Forum of 2012 an example of successful cooperation for the advancement of political, military and security interests.[3]

Such security arrangements are clearly necessary given that many GCC countries have experienced armed conflict in recent decades: the Iran-Iraq War in 1980, the Iraqi invasion of Kuwait in 1990, the US-led invasion of Iraq in 2003, and the ongoing war in Yemen all highlight the absence of a GCC security and defence arrangement which is powerful enough to deter or resolve regional disputes.

The problem lies in the nature of the GCC as an economic and political grouping, with little appetite for closer cooperation in the fields of security, conflict prevention or defence. Its founding document, the GCC Charter, was ratified in May 1981 and requires cooperation in financial and economic interests, customs, education and culture, as well as administrative procedures between member-states.[4] However, there is no provision for external security or defence arrangements.

A planned GCC Internal Security Pact, as a successor to the failed Internal Security Agreement of 1982, focuses more on internal challenges and has been criticised for its potential to be used as a tool of internal persecution.[5] The findings of the Doha Declaration of 1990, which highlighted the ineffectiveness of GCC defence and security arrangements, are still valid.[6] While a number of GCC countries have bilateral defence agreements, there is no doubt that addressing these concerns in the GCC Charter could strengthen the GCC and regional security.

The Second Lebanon War 2006 as a precursor of hybrid threats/warfare

Hybrid warfare is an emerging notion of 21st century conflict that combines four elements along the spectrum of warfare, namely conventional warfare, irregular warfare (terrorism and counter-insurgency), asymmetric warfare (waged by resistance groups) and compound warfare (wherein irregular forces supplement a conventional force).[7]

As a potentially new method of warfare, it expands on existing doctrinal elements in three ways: firstly, by furthering unconventional warfighting capacities alongside conventional methods but beyond the existing compound (spectrum) operations, such as cyber-warfare; secondly, by pursuing activities in the so-called 'information sphere' and, thirdly, by using 'lawfare' to achieve political and strategic objectives.[8]

The use of hybrid warfare in the Middle East became recognised during the Lebanon War in 2006, when Hezbollah fought a multifaceted campaign against Israel, blending conventional (the use of rocket bombardments of northern Israel and employing robust anti-tank warfare against Israeli armour) with unconventional methods (such as the use of improvised explosive devices) and cyber-based operations (such as the sending of text messages of an official character to Israeli mobile phone users notifying them of the false death of a soldier on the front).[9] Frank Hoffman described Hezbollah's methods as constituting both hybrid threats and hybrid warfare.[10]

More recent examples include Russia's involvement in the conflict in Ukraine, and IS operations

in Iraq and Syria, as well as its recent recruitment and radicalisation campaigns in EU countries for the 'jihad' in Syria and 'martyrdom' operations in Europe. These examples use a holistic mix of conventional and non-conventional forms of warfare, information operations, lawfare and cyber-attacks, aimed at testing the resilience of the affected states and societies. The way the current GCC crisis has unfolded allows for some comparison with these conflicts and how methods of hybrid warfare are being employed to exploit vulnerabilities and lack of resilience, both as measures and countermeasures.

As early as 2010, NATO identified 'hybrid threats' as low-intensity, kinetic and non-kinetic threats to international peace and security, including cyber war, low-intensity asymmetric conflict scenarios, global terrorism, piracy, transnational organised crime, demographic challenges, resources, security, retrenchment from globalisation, and the proliferation of weapons of mass destruction.[11]

One such type of hybrid threat is cyber threats, which constitute threats in the 'fifth dimension' of warfare, as cyberwarfare is often described.[12] Cyber threats refer to sustained campaigns of concerted cyber operations against the IT infrastructure of a targeted state, including mass web disruption, spam use and malware infection.[13]

While cyber-attacks do not involve the use of force *per se*, their effects in terms of loss of life and material damage to property may be comparable to the effects of an armed attack. Indeed, the *Tallinn Manual*, authored by a panel of international experts and published by NATO's Cooperative Cyber Defence Centre of Excellence in 2013, contends that cyber-attacks, if they cause death, injury or damage, can be regarded as the use of force.[14]

Cyber-attacks can therefore constitute a method of warfighting *sui generis*, as evident in Russia's cyber-attack on Estonia in 2009, or as part of a conventional military campaign in a supporting role and function. The use of cyber as a force multiplier was also evident in Russia's use to augment its military capabilities during its military campaigns against Georgia in 2008, and more recently in Ukraine since 2014.[15]

Between 2010 and 2012, NATO—recognising hybrid threats as a major risk—began work to identify these threats and define a comprehensive approach for countering them by including state and non-state actors in a comprehensive defence strategy. According to NATO's

Bi-Strategic Command Capstone Concept of 2010, hybrid threats represent complex and non-linear threats that are difficult to resolve using one-dimensional measures such as military action.[16] Specifically, hybrid threats are defined by NATO as 'those threats posed by adversaries with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives'.

Perhaps short-sightedly, given Russia's aggression in Eastern Europe, this project was discontinued in 2012 due to lack of support from NATO members. However, in December 2015, NATO announced the development of a new *Hybrid Warfare Strategy* which, in essence, recognises the existing capstone document of 2010 as a blueprint for countering hybrid threats 'in a comprehensive way [and] in the complex geostrategic environment posed by globalisation'.[17] That clearly was in response to events in Ukraine and Russia's annexation of Crimea, in which Russia used security, military, political, legal, informational, technical and economic means to advance its interests.

Another element of hybrid warfare can be the use of 'lawfare', the use of law as a weapon.[18] Russia has succeeded in using law as a means of warfare in its movement into Crimea, as the absence of a clear definition of the nature of 'intervention' has made the action difficult to categorise in international law. As a result, in addition to Russia's denial of these actions, the legal assessment in terms of legality/illegality has become a partisan undertaking.[19] What has become clear is that countering hybrid threats/ warfare will shape NATO's future role in addressing armed conflict and global risk and crisis management.

Recent cyber-attacks in the Gulf as a precursor to the current crisis

Even before the current crisis, Qatar and other GCC states recognised their vulnerability to cyber-attacks on their critical infrastructure, not least because of prior attacks directed against Qatar and Saudi Arabia. In 2015, Qatar's Minister of Information and Communication Technology asserted that protecting the nation's critical infrastructure is a key objective of its cybersecurity policy:

> Qatar has taken steps for transitioning from a traditional hydrocarbon-based economy to a digital economy…. However, digital inter-connectedness is only beneficial if we can ensure our citizens and businesses are safe in the digital world that we are transitioning to a digital government.[20]

Security experts have hinted that Qatar may face a high risk of cyber-attacks as the host of the upcoming FIFA 2022 World Cup, cautioning that the nation's financial, oil and gas sectors continue to be vulnerable to cyber-attacks.[21] Indeed, an increasing number of cyber-attacks have recently been reported in the Gulf. In 2012, Qatar's second-largest liquefied natural gas producer, RasGas, was attacked by Shamoon, a computer virus that caused its system to go offline.[22] Earlier, in 2010, it was reported that a sophisticated virus/worm called Stuxnet had been used, allegedly by Israel and/or the US, to sabotage Iran's nuclear weapons program.[23]

This vulnerability and the occurrence of such attacks makes Qatar (and other GCC states) an interesting case study for examining the nature and form of cyber-attacks in terms of the *Tallinn* guidelines, and as a form of hybrid threat or a method of hybrid warfare. With its vast reserves of natural resources and critical infrastructure, and its strategic position in the Persian Gulf, Qatar is particularly vulnerable to cyber and hybrid attacks.

The Saudi Arabian Oil Company)ARAMCO) was hacked in 2015, an act that has been described as one of the most severe in the history of the GCC.[24] The impact of this cyber-attack and its exploitation of network-related vulnerabilities shook the confidence of Saudi Arabia's global business partners and contractors of ARAMCO. The GCC position has been that this attack originated from or on behalf of Iran, and led to a consensus of how to improve resilience and develop counter-attack options in the future. That leads to the question of whether other GCC states would have protected each other in such instances prior to the current GCC crisis, given the lack of a regional defence consensus or arrangement.

The use of hybrid warfare in the current Qatar-GCC crisis

In early June 2017, three GCC member states (Saudi Arabia, UAE and Bahrain) cut diplomatic ties with Qatar, imposed a trade embargo, and expelled Qatari nationals from their territories, as well as banning any travel to Qatar. These measures were justified as constituting a legitimate response and countermeasure to Qatar's continuing support for terrorist organisations in the region.[25]

The boycott/embargo was supported by several regional but non-GCC states, such as Egypt, Jordan, Yemen and other countries that are generally seen to follow or be influenced by GCC countries. The ensuing crisis was further escalated by President Trump's statement on Twitter that Qatar 'has been a funder of terrorism at a very high level', which directly contradicted Secretary of State Tillerson's attempts to ease tension in the region.[26]

The present anti-Qatar policy is a model mix of 'diplomatic, information, military, and economic' actions, targeting political, military, economic, social, information and infrastructure effects.[27] The Saudi and UAE-led blockade was supported by classical 'soft power' action, notably Saudi Arabia's decision to close its land border with Qatar, the only land border of the Qatari peninsula. The 'blockade' countries have also blocked their respective air space for any air travel to and from Qatar.

The blockade policy by Saudi Arabia and UAE, utilising a means short of the use of force, falls within the operational spectrum of hybrid warfare. Given that the blockade has been augmented by other supporting action, which also falls under the wider umbrella of hybrid warfare, it seems appropriate to view the current GCC situation as falling within the wider hybrid warfare/hybrid threats warfare spectrum. Other examples include exercising direct pressure on religious leaders in Qatar, and the use of the international media and information sphere to support Saudi Arabia's narrative of Qatar's terrorism links, as well as the attempt to use Arab writers, intellectuals and tribal leaders to take a stance against Qatar's government.

The blockade of Qatar's sea, land and air borders prevented Qatari citizens from entering or leaving the country. They were also forced to leave the affected states (and Saudi and UAE citizens residing in Qatar were forced to leave Qatar in response to pressure from their home countries). These actions, which violate both international law and GCC law, have surprised both the Qatari people and their government, particularly given the close links within GCC member-states along and across tribal and family lines.

Saudi Arabia's decision also to send back camels (and sheep) from Saudi Arabia to Qatar has hit a particular raw nerve in the Arab nation due to its cultural attachment to camels.[28] Camels are not only the main means of transport in the region but are synonymous with the region's pre-petroleum wealth. Saudi Arabia also imposed conditions on pilgrims from Qatar arriving in the country for the annual Hajj of 2017, which was more-widely condemned as affecting their freedom of religion.[29]

The current crisis commenced with a cyber-attack targeting the Qatar News Agency and the uploading of fake news involving statements allegedly made by the Emir of Qatar (which he later accused some of the embargoing countries of using as a pretext to carry out the blockade).[30] *The Washington Post* reported in mid-July that the UAE may have been behind this cyber operation.[31]

The Gulf states' campaign against Qatar has the hallmarks of a hybrid warfare campaign, combining a variety of non-kinetic means and tools, including information operations, economic and diplomatic blockade, and cyber operations. Missing so far has been the use of covert operatives, so-called local volunteers and other non-attributable operatives, to escalate the conflict to the next stage, which would turn the present crisis into a fully-fledged hybrid warfare campaign comparable to Russia's Crimea campaign of 2014.

The use of hybrid warfare is not new to the GCC. Another example of such multi-modal hybrid warfare could be seen in the Bahraini protests of 2011. Bahrain has a population of various religions and sects (predominantly Sunni and Shia). In 2011, demonstrators in Bahrain demanded improved economic conditions and human rights. What began as a local protest became a hybrid threat when peaceful gatherings turned into a sectarian protest of the Shia minority against the rule of the Sunni Emir. The protestors were edged on by Shia leaders from Iran and its Lebanese affiliate Hezbollah, media outlets in Iran, and Hezbollah-supported protestors on the ground.

This turned the original protests into a Sunni-Shia conflict, with an increase in violence originating from domestic and outside actors aimed at the government of the state. The situation became so volatile that Bahrain had to ask for military assistance from a Saudi-led GCC coalition. This could be considered an example of hybrid warfare, as internal unrest was turned into a regional security threat with the support of an external state (Iran) and its non-state affiliates. Iran, while denying any interest and involvement, used diplomacy, media operations and eventually lawfare to support the unrest in a fashion used successfully by Russia three years later in Crimean.[32]

Conclusion

It seems that the Gulf states continue to be vulnerable to both unconventional warfare and hybrid attacks alike, whether originating from GCC states, other states or non-state actors. The only solution would seem to lie in the development of an effective GCC defence arrangement, rather than the continuation of unilateral efforts—which create vulnerabilities on their own and often lead to an increase in mutual distrust among the GCC nations. It is also clearly important, both for regional and broader global stability, that the situation returns to a pre-crisis status quo.

Qatar's answer to the current crisis is not an easy one. Indeed, given the quantity and quality of the hybrid warfare campaign being targeted at it, the response will require an equally comprehensive approach combining diplomacy, lawfare, information operations and economic countermeasures. The question remains, which countermeasures should Qatar employ and what would be the ramifications. For example, were Qatar to use Al Jazeera more aggressively, as a propaganda tool in the information sphere, how would that play out? Could it escalate or deescalate the situation?

Similarly, if Qatar were to deploy cyber countermeasures against Saudi Arabia, what could be achieved and how would this play out in terms of achieving the overall objective of resolving the present crisis? Is Qatar, realistically, able to do very much, apart from sticking to the lawful response through lawfare? The Charter of the GCC may be the legislative instrument to address this situation. However, to date, the Charter has largely only dealt with administrative matters. So attempting to elevate the Charter to security issues may put the cooperative future of the GCC at stake.

At present, Qatar seems inclined to utilise hybrid countermeasures, using 'lawfare' in the wider sense, by making a legal complaint to the World Trade Organization over the economic blockade, and complaining to the International Civil Aviation Organization, albeit without success to date.[33] It has also increased its production of liquid gas by 30 per cent as an economic countermeasure, as well as utilising trade and diplomacy as strategic leverage.[34]

Given the continuing strategic relevance of the GCC region for US and European foreign policy, the re-emergence of the threat posed by Iran, and the need to reduce tensions among GCC member-states in order to maintain US (and other) strategic interests in terms of trade and strategic cooperation, it seems likely that the crisis will be resolved in the not too distant future. In the meantime, it is a good example of the broadening use and prospective success of hybrid warfare.

Sascha-Dominik Dov Bachmann is an Associate Professor in International Law at Bournemouth University (UK) and Associate Professor in War Studies at the Swedish Defence University. As a reservist in the German Army, he served in peacekeeping missions in an operational and advisory capacity. He took part as NATO's 'rule of law subject-matter expert' in NATO's 'Hybrid Threat Experiment' of 2011 and in related workshops at NATO and national level. He has widely written on the subject of hybrid threats/warfare and lawfare from an operational perspective.

Notes

1 See P. Danahar, *The New Middle East: the world after the Arab Spring*, Bloomsbury: London, 2013 for an authoritative introduction and discussion of the term within its political and historical context.

2 Trading Economic, 'Crude oil production', *Trading Economic* [website], available at <https://tradingeconomics.com/country-list/crude-oil-production> accessed 18 July 2017; *Arab News*, 'GCC share of global oil reserves likely to raise to 70%', *Arab News* [website], available at <http://www.arabnews.com/gcc-share-global-oil-reserves-likely-rise-70> accessed 18 July 2017.

3 See, for example, the British position highlighted in *Al Jazeera*, 'Britain to deepen security cooperation with the GCC', *Al Jazeera* [website], 7 December 2016, available at <http://www.aljazeera.com/news/2016/12/britain-deepen-security-cooperation-gcc-161207102311180.html> accessed 18 July 2017; see also *SUSRIS,* 'US-GCC Strategic Cooperation Forum', available at <http://susris.com/glossary/us-gcc-strategic-cooperation-forum/> accessed 18 July 2017.

4 For an English version, see International Relations and Security Network (SRN), 'Charter of the Gulf Cooperation Council (GCC)', *SRN* [website], available at <https://www.files.ethz.ch/isn/125347/1426_GCC.pdf> accessed 20 July 2017.

5 See Human Rights Watch, 'GCC: joint security agreement imperils rights', *Human Rights Watch* [website], 26 April 2014, available at <https://www.hrw.org/news/2014/04/26/gcc-joint-security-agreement-imperils-rights> accessed 20 July 2017.

6 See, for example, C. Koch, 'The GCC as a regional security organization', *KAS International Reports* [website], <http://www.kas.de/wf/doc/kas_21076-544-2-30.pdf?101110135754> accessed 18 July 2017.

7 S.D. Bachmann and A.B.M. Mosquera, 'Lawfare and hybrid warfare –how Russia is using the law as a weapon', *Amicus Curiae*, Issue 102, 2015, abstract available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2841277> accessed 17 July 2017.

8 S.D. Bachmann and H. Gunneriusson, 'Eyes wide shut: how Russia's hybrid warfare exposes and exploits Western vulnerabilities', *Georgetown Journal of International Affairs*, 18 January 2017, available at <http://journal.georgetown.edu/eyes-wide-shut-how-russias-hybrid-warfare-exposes-and-exploits-western-vulnerabilities/> accessed 17 July 2017.

9 F.G. Hoffman, *Conflict in the 21st century: the rise of hybrid wars*, Potomac Institute for Policy Studies: Arlington, 2007, p. 37.

10 Hoffman revisited his discussion of the hybridity of Hezbollah's warfighting approach in subsequent academic works where he discussed the interchangeable nature of the terms hybrid threats and warfare. See, for example, F.G. Hoffman, 'Hybrid warfare and challenges', *Joint Forces Quarterly*, Issue 52, 1st Quarter 2009, pp. 1-2; and F.G. Hoffman, 'Hybrid vs. compound war: the Janus choice of modern war: defining today's multifaceted conflict', *Armed Forces Journal*, October 2009, pp. 1-2.

11 S. Bachmann, 'Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats—mapping the new frontier of global risk and security management', *Amicus Curiae*, Issue 88, January 2012; and NATO, 'NATO countering the hybrid threat', *NATO* [website], available at <http://www.act.nato.int/nato-countering-the-hybrid-threat> accessed 17 July 2017.

12 S. Bachmann and H. Gunnariusson, 'Russia's hybrid warfare in the East: the integral nature of the information sphere', *Georgetown Journal of International Affairs*, 2015, pp. 198-212.

13 S. Bachmann and H. Gunnariusson, 'Hybrid wars: the 21st century's new threats to global peace and security', *South African Journal of Military Studies*, Issue 43, No. 1, 2015, pp. 77-98.

14 See the latest edition at Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2017, available at <https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html> accessed 25 January 2018.

15 Bachmann and Gunneriusson, 'Eyes wide shut'.

16 P. Fleming, 'The hybrid threat concept: contemporary war, military planning and the advent of unrestricted operational art', *Homeland Security Digital Library* [website], available at <https://www.hsdl.org/?view&did=700828/> accessed 17 July 2017.

17 NATO, 'Press statements by the NATO Secretary General Jens Stoltenberg and the EU High Representative for Foreign Affairs and Security Policy, Federica Mogherini, 1 December 2015', *NATO* [website], available at <http://www.nato.int/cps/en/natohq/opinions_125361.htm> accessed 17 November 2015.

18 S.D. Bachmann and A.B.M. Mosquera, 'Lawfare in hybrid wars: the 21st century warfare', *Journal of International Humanitarian Legal Studies*, Issue 7, 2016, p. 63, with reference to Dunlap who coined the term in 2001.

19 S.D. Bachmann and A.B.M. Mosquera, 'Lawfare and hybrid warfare –how Russia is using the law as a weapon', *Amicus Curiae*, Issue 102, 2015.

20 H. al-Jaber, 'Protecting critical infrastructure key to Qatar's cyber security approach', *Gulf Times* [website], 19 April 2015, available at <http://www.gulf-times.com/qatar/178/details/435549/%E2%80%98protecting-critical-infrastructure-key-to-qatar%E2%80%99s-cyber-security-approach%E2%80%99> accessed 23 November 2015.

21 Aarti Nagraj, 'Qatar faces high risk of cyber-attacks during FIFA 2022 World Cup', *Gulf Business* [website], 23 April 2015, available at <http://gulfbusiness.com/qatar-faces-high-risk-cyber-attacks-fifa-2022-world-cup/> accessed 24 November 2015.

22 *The New Arab*, 'GCC businesses are facing a major cybersecurity deficit', *The New Arab* [website], 12 June 2017, available at <https://www.alaraby.co.uk/english/comment/2017/6/12/gcc-businesses-are-facing-a-major-cybersecurity-deficit> accessed 3 June 2017; P. Paganini, 'RasGas, new cyber-attack against an energy company', *Security Affairs* [website], 31 August 2012, available at <http://securityaffairs.co/wordpress/8332/malware/rasgas-new-cyber-attack-against-an-energy-company.html> accessed 3 August 2017.

23 C. Williams, 'Stuxnet: cyber-attack on Iran "was carried out by Western powers and Israel"', *The Telegraph*

[website], 21 January 2011, available at <http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.htm> accessed 25 January 2018.

24 J. Pagliery, 'The inside story of the biggest hack in history', *CNNMoney* [website], 5 August 2015, available at <http://money.cnn.com/2015/08/05/technology/aramco-hack/index.html> accessed 20 July 2017.

25 For a short overview, see *BBC News*, 'Qatar crisis: what you need to know', *BBC News* [website], 5 July 2017, available at <http://www.bbc.co.uk/news/world-middle-east-40173757> accessed 3 August 2017.

26 *The Guardian*, 'Gulf crisis: Trump escalates row by accusing Qatar of sponsoring terror', *The Guardian* [website], available at <https://www.theguardian.com/us-news/2017/jun/09/trump-qatar-sponsor-terrorism-middle-east> accessed 20 July 2017.

27 R. Hillson, 'The DIME/PMESII Model Suite Requirements Project', *NRL Review* [website], available at <https://www.nrl.navy.mil/content_images/09_Simulation_Hillson.pdf> accessed 20 July 2017.

28 Bethany Allen-Ebrahimian, 'Saudi Arabia deports 15,000 Qatari camels', *Foreign Policy* [website], 20 June 2017, available at <http://foreignpolicy.com/2017/06/20/saudi-arabia-deports-qatari-camels-gulf-diplomacy/> accessed 20 July 2017.

29 The Euro-Mediterranean Human Rights Monitor, 'New report: travel restrictions on Qataris seeking to perform religious rituals in Saudi Arabia is serious violation that requires investigation', *The Euro-Mediterranean Human Rights Monitor* [website], 21 November 2017, available at <https://euromedmonitor.org/en/article/2180/New-report:-Travel-restrictions-on-Qataris-seeking-to-perform-religious-rituals-in-Saudi-Arabia-is-serious-violation-that-requires-investigation> accessed 25 January 2018.

30 See, for example, R. Windrem and W. Arkin, 'Who planted the fake news at center of Qatar crisis', *NBC News* [website], 18 July 2017, available at <http://www.nbcnews.com/news/world/who-planted-fake-news-center-qatar-crisis-n784056> accessed 20 July 2017.

31 Karen DeYoung and Ellen Nakashima, 'UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to US intelligence officials', *Washington Post* [website], 16 July 2017, available at <http://wapo.st/2tvcnXx?tid=ss_tw&utm_term=.2c9ddcf63846> accessed 20 July 2017.

32 M. Slackman, 'The proxy battle in Bahrain' *The New York Times* [website], 19 March 2011, available at <http://www.nytimes.com/2011/03/20/weekinreview/20proxy.html> accessed 25 January 2018.

33 Reuters, 'Qatar makes legal complaint over Gulf trade boycott', *The Guardian* [website], 1 August 2017, available at <https://www.theguardian.com/world/2017/jul/31/qatar-makes-legal-complaint-to-wto-over-gulf-trade-boycott> accessed 25 January 2018.

34 Reuters, 'Qatar announces huge raise in gas production amid diplomatic crisis', *CNBC* [website], 4 July 2017, available at <https://www.cnbc.com/2017/07/04/qatar-ratchets-up-gas-production-30-percent-despite-sanctions.html> accessed 25 January 2018. See also The Associated Press, 'Seeking closer ties, Qatar to expand base used by US troops', *Military.com* [website], 1 February 2018, available at <https://www.military.com/daily-news/2018/02/01/seeking-closer-ties-qatar-expand-base-used-us-troops.html> accessed 5 February 2018; and UK Ministry of Defence, 'Defence Secretary signs multi billion pound jet contract with Qatar', *Ministry of Defence* [website], 7 December 2017, available at <https://www.contracts.mod.uk/do-features-and-articles/defence-secretary-signs-multi-billion-pound-jet-contract-with-qatar/> accessed 5 February 2018.