The Political Economy of Communication
6(1), 3–35

http://www.polecom.org

A New Kind of Information Warfare? Cyber-conflict and the Gulf crisis 2010–2017

Tarek Cherkaoui, TRT World Research Centre

Keywords: Information warfare, information operations, information dominance, propaganda, disinformation, political warfare, media warfare, cyber warfare, hacktivism, cyber-terrorism.

Abstract

This article analyses the current Gulf crisis that started in May 2017 by posing the following question. Did an information war unfold or did the crisis events that took place merely illustrate yet another round of propaganda and disinformation contests among Gulf participants and their backers? Accordingly, I will focus on five central themes. First, the theoretical underpinning and key concepts concerning Information Warfare (and related notions like Hacktivism and Cyber War) will be discussed in relation to information space and the media sphere. The second theme explores the historical, strategic, and geopolitical dynamics that led to the crisis and looks closely at the rivalries taking place in the region, with a particular focus on the proxy war between Iran and Saudi Arabia. Against a backdrop of geopolitical tensions and cyber threats, the third theme reviews some of the most notorious cyber attacks that occurred in the Gulf region up until the Trump Presidency. The fourth theme sheds some light on recent manifestations of the Gulf crisis and the anti-Qatar coalition's modus operandi. Fifthly, Qatar's response to the crisis will be reviewed and evaluated.

The 2003 War on Iraq has altered the balance of power in the Middle East, and the Gulf region has been in the throes of change since then. The situation became even more complicated with another defining historic moment, namely the Arab Spring, which triggered more profound disagreements in the Gulf, and divided its governments into two antagonistic camps. The Qatari leadership sided with the Arab uprisings, and Al Jazeera played a leading role in conveying these events to millions of Arab and international viewers around the globe, thus facilitating popular demands for democracy and civil rights. The other camp, which is led by the rulers of Saudi Arabia, the United Arab Emirates (UAE), and Egypt (henceforth 'the quartet'), viewed this chapter as a threat to their authority and a menace to their regional geopolitical posture. Tensions brewed for a few years between both parties and reached a climax in the spring of 2017 when the quartet countries subjected Qatar to a blockade.

As indicated, the fundamental purpose of this article is to ascertain the distinctiveness or otherwise of Information War (IW) in regard to the Gulf crisis. To this end, the theoretical paradigm underpinning IW will be reviewed, and some of the 21st century's effective models will be outlined. Since some of the protagonists have been building cyber-warfare capabilities over the past decade, an analysis of the cyber-infiltrations and cyber-attacks in the region, both linked to state and non-state actors, is warranted. At the same time, tensions in the Gulf region over the past year have developed on several fronts: diplomatic, political, economic, military, media, and cyberspace. All of these fronts will be carefully examined.

On Information Warfare

The 1991 Gulf War highlighted the importance of Information Warfare (IW) [1]. It was then that the American military waged a cyber war, establishing cyberspace as the fifth and most recent domain of war (preceded by land, sea, air, and space) (Schreier, 2015). IW has been defined as "a targeted effort to undercut and neutralise the enemy's command and control system for the purpose of protecting and coordinating the activities of the command and control system of friendly forces" (Blair, 2001 cited in Damjanovic, 2017: 1045). This general strategy includes a panoply of measures, including espionage, undermining the enemy's information, preventing the enemy from accessing information, and spreading propaganda and disinformation to demoralise or manipulate the opponent and the public (Reisman and Antoniou, 1994).

The jump into the information and communication technology revolution made cyber warfare an essential component of IW measures. Author Fred Schreier understood cyber warfare as the "deliberate action to alter, disrupt, deceive, degrade, or destroy computer systems and networks or the information and/or programs resident in or transiting these systems or networks" (Schreier, 2015: 68). Such definition avoids those generalisations that tend to include cyber-crimes and online delinquencies under the umbrella of cyber war or attack.

Conceptually, this article is aligned with Schreier's proposition that cyber war is a subsection of Information Warfare. In essence, IW includes five core capabilities: (1) Psychological Operations, (2) Military Deception, (3) Operations Security, (4) Computer Network Operations (CNO), and (5) Electronic Warfare (2015: 21). According to Schreier, the fourth of these, CNO, includes "the capability to attack and disrupt computer networks, defend their own information and communications systems, and exploit enemy computer networks through intelligence collection, usually done through the use of computer code and computer applications" (2015: 20). Moreover, Schreier argues that "cyber war means disrupting or destroying information and communications systems. It also means trying to know everything about an adversary while keeping the adversary from knowing much about oneself… As in other forms of warfare, cyber war aims at influencing the will and decision making capability of the enemy's political leadership and armed forces in the theatre of Computer Network Operations (CNO)" (2015: 26).

The strong deployment of IW in Desert Storm during the 1991 Gulf War paved the way for additional control over information during conflicts, leading to the emergence of the "information dominance" paradigm. Jim Winters and John Giffin, of the U.S. Space and Information Operations Directorate, provided the rationale. In their opinion, the U.S. armed forces "face a threefold asymmetry problem on any future battlefield - asymmetry of threat, asymmetry of technology, and asymmetry of information. In any one of these areas denotative superiority may not be sufficient. Information dominance presents the only conceptual basis for prevailing in spite of these potential

asymmetries" (Winters and Giffin, 1997). According to this perspective, information dominance is a central component of the U.S. aim of total spectrum dominance. "When dominance occurs, nothing done makes any difference. We have sufficient knowledge to stop anything we do not want to occur, or do anything we want to do" (Winters and Giffin, 1997).

Academic and intelligence expert Douglas Dearth offered further elaboration. For him, the first function of information dominance, "perception management", shapes the information space and is an organising principle of policy and the application of power in the international arena. Perception management involves "actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives and objective reasoning. It also enables "intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviours and official actions favourable to the originator's objectives" (Dearth, 2002: 2). This takes place concurrently in both international politics and conflict situations, and involves both "truth-telling" and "truth-corrupting" over a wide range of areas by jointly combining soft power (e.g. political power, economic power, public affairs, public diplomacy) and physical elements, whether actively or as a deterrent (e.g. psyops, deception, covert actions, deterrent capabilities). The general purpose is to ensure the dominance of a specific interpretation of reality (2002: 2, 8). Dearth acknowledges that many of these activities have been undertaken before, but argues that they have not been employed in proper synergy since the Second World War. Furthermore, earlier employments of perception management did not have access to modern forms of information and communications technology (ICT).

Dearth also outlined the second function of information at the intermediate level, which is to shape the conflict space. Again, this occurs through both soft and hard power methods, such as international power projection, force disposition, covert actions, in addition to forms of public diplomacy and public affairs. The author contextualised this level by discussing U.S. peacekeeping roles, where the Pentagon had to shape the conflict space and did so by having sufficient power projection and strength on the ground to prevent battles from taking place (2002: 8-9). He also elaborated on the third level, namely, shaping the battle space. This endeavour is more tactically oriented and is primarily concerned with the deployment of firepower within a delimited physical space – land, sea or air – in order to gain a material and positional advantage. For him, non-physical elements of power contribute to this task, but they are generally of secondary importance (2002: 8).

The information dominance approach was tested during the 2003 Iraq War, prompting armed forces around the world to emulate it, and integrate the lessons learned into their modes of warfare. Strategies of IW were integrated, from the outset, into the core of military strategy (Miller, 2003). In parallel to these military developments, emerging non-state actors took advantage of the information revolution, and started carrying out computer network attacks, hacking, and data theft.

Hacktivism [2], which constitutes a marriage between political activism and computer hacking (Denning, 1999), is viewed with extreme distrust by officialdom and law enforcement agencies. This form of cyber activism could be regarded as the 'war of the flea' within cyberspace, whereby big entities suffer the dog's disadvantages: too much to protect in the face of an adversary that is hidden, small, and swift. Hungarian academic Sandor Vegh succinctly defined hacktivism as "a politically motivated single incident online action, or a campaign thereof, taken by non-state actors in retaliation to express disapproval or to call attention to an issue advocated by the activists" (Vegh, 2003: 83). Some researchers consider the rise of hacktivism as a radical consequence of globalisation, which explains its anti-corporate and anti-capitalist manifestations (Taylor, 2001). It has also been asserted

that hacktivists vie to utilise the power of the Internet to seek international publicity and establish alliances with like-minded groups and individuals (Norris, 2001).

One of the most widely known hacktivist collectives is Anonymous, which became known to the broader public through their Distributed Denial of Service (DDoS) attacks in solidarity with WikiLeaks in December 2010. These actions were responsible for shutting down the websites of PayPal, PostFinance, Visa, MasterCard, and the Bank of America, as these financial institutions discontinued the possibility of sending money to WikiLeaks (Fuchs, 2014). According to academic Christian Fuchs, Anonymous' ideology blends several political persuasions, such as "anarchism, liberalism, communism, and libertarianism" (ibid: 345). While this collective has been depicted in academia as "cyber-vigilantes" (Serracino-Inglott, 2013: 221), another perspective portrayed its adherents as extraordinary bandits (e-bandits) since they follow the footsteps of Robin Hood by empowering the disempowered in their attempt to keep the Internet free (Wong and Brown, 2013: 1015, 1018).

WikiLeaks, which was established in 2006, consider themselves as enablers who empower the oppressed by offering them access to critical information. There are numerous similarities between Anonymous and WikiLeaks. Both organisations operate in secrecy; have a global reach, target corporations and governments in an unprecedented way, and function structurally as networks to avoid receiving a deadly blow from authorities (1018). WikiLeaks' goal is to seek and publish secrets and confidential information from whistle-blowers worldwide (CBS, 2011). They also offer a very high level of protection and anonymity to their sources, making the traceability and censorship of their documents, or shutting down their operations virtually impossible (Sutter, 2010).

WikiLeaks came into the limelight when it released a video that showed a U.S. Apache helicopter opening fire on a Baghdad street in April 2010 and killing many bystanders including two journalists from Reuters (CBS, 2011). They then released 76,000 classified documents on the U.S. operations in Afghanistan, and 400,000 confidential papers on the Iraq war, which revealed a systematic cover-up of civilian casualties. In November 2010, they leaked thousands of State Department cables, which exposed several U.S. espionage operations targeting high-level personalities at the United Nations (ibid.). The magnitude of the revelations led high-level U.S. officials like former Vice President Joe Biden to call the WikiLeaks founder Julian Assange a "high-tech terrorist" (MacAskill, 2010).

In an internal report issued in 2008, U.S. Army intelligence cautioned against possible risks arising from WikiLeaks actions and stated that the collective "poses a significant 'operational security and information security' threat to military operations" (McCullagh, 2010). The report warned that the potential leaking of secret U.S. military documents by WikiLeaks could "influence operations against the U.S. Army by a variety of domestic and foreign actors," while a section of the document says that WikiLeaks is "knowingly encouraging criminal activities," including violation of national security laws regarding sedition and espionage (McCullagh, 2010).

Increasingly, non-state actors around the world have acquired capabilities that could potentially threaten national security. These organisations are adept at using the Internet and can launch organised propaganda and disinformation campaigns, while also mounting various intrusions and cyber attacks on states' critical infrastructure and key assets. In a report commissioned by the Department of Defence (DoD), the U.S. Director of National Intelligence in 2015 designated the cyber attack, rather than terrorism, as the number one strategic threat to the United States for the first time since the attacks of September 11, 2001 (Department of Defence, 2015a: 9).

The DoD report identified a variety of threats, such as disrupting "an organisation's operations for activist purposes," stealing intellectual property, and conducting "disruptive and destructive

attacks to achieve military objectives" (2015a: 9). The document also named potential adversaries such as Russia, China, Iran, and North Korea, even if the latter two have "less developed cyber capabilities"(2015a: 9). The report mentioned non-state actors like the Islamic State in Iraq and the Levant, and observed that "state and non-state threats often also blend together; patriotic entities often act as cyber surrogates for states, and non-state entities can provide cover for state-based operators" (2015a: 9).

The documents mentioned here reflect a sense of urgency even when the Pentagon has maintained information dominance over all other adversaries. It is heavily investing in futuristic and state-of-the-art technologies, such as advanced computing, big data, and human-machine teaming (Department of Defence, 2015b). Arguably, the tendency to over-rely on ICT capabilities and the development of weapon systems that are entirely dependent on computers may have turned such advantage into a vulnerability; especially when various state and non-state actors have invested in low-cost methods to stage highly-organised and potent cyber attacks. U.S. Secretary of Defence Leon Panetta expressed such concern when he warned about a "Digital Pearl Harbor." For him, the "next Pearl Harbor we confront could very well be a cyber attack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems" (Lieberman, Collins, and Carper, 2011: 1).

In short, cyber warfare is a subset of IW and falls under Computer Network Operations. It aims to disrupt or destroy the enemy's information and communications systems, while also preventing the enemy from inflicting similar damage. In contrast, hacktivism is a form of irregular disruption in cyberspace, which is conducted by individuals or groups to advance their political agendas. The increase in capabilities at both state and non-state level has created real vulnerabilities for established powers and added more complexity to the already complex state of international affairs.

History and hegemony in the Gulf

In the Gulf region, some of the conflicts are deeply rooted in history. Qatar, for instance, has been living since the 18th century under the menace of the tribes governing neighbouring Saudi Arabia, Bahrain, and the Trucial Sheikhdoms (currently the United Arab Emirates (UAE)). The country was thus obliged to acknowledge the authority of the Saudis as early as 1797; the latter's use of force enabled them to rise above the narrow circumference of their early settlement in the Najd region (al-Rasheed, 2002: 19, 21). Britain's intervention in the Gulf - starting from 1835 - had put in place a security architecture for the region, and laid the foundation for Pax Britannica (Onley, 2009: 1). After Britain's withdrawal from east of Suez in 1971, Saudi Arabia seized the moment to coerce its neighbours and grab disputed territories from Abu Dhabi and Oman (Hellyer, 2001: 167). Qatar was considered a backwater Saudi vassal state (Hammond, 2014: 2).

This situation lasted until the Saddam Hussein's invasion of Kuwait, which threatened Saudi Arabia's sovereignty as well. When Riyadh called for U.S. military assistance, it became apparent that Saudi Arabia was merely a paper tiger, and that small states in the region had to look elsewhere for protection. This conflict signalled a shift in Saudi—Qatari relations, and Doha took a significant decision by signing military agreements with the U.S., which allowed them to establish one of their most important air bases in the region. Ensuing tensions between Saudi Arabia and Qatar lead to border skirmishes, which left three Qatari troopers dead on 30 September 1992. Other low-intensity clashes were observed in 1994. The Saudis also exerted economic pressure when they blocked Qatari

plans to export its gas via land routes to other Gulf Cooperation Council (GCC) countries (Roberts, 2012).

Consequently, Qatar had to find strategies that would avoid Saudi domination. First, the Qatari leadership looked to capitalise on the nation's vast resources (third-largest reserves of natural gas in the world) while bypassing Saudi control over the sole road passage out of the region. Therefore, Doha decided to export liquefied natural gas (LNG) to the world through maritime routes. This led to the establishment of an advanced LNG infrastructure (QNB, 2015), making Qatar the world's largest gas exporter (Energy Information Administration, 2015).

The vast revenues that entered Qatar's treasury turned the country into one of the world's wealthiest nations, with an annual per-capita income of $130,000 (2011). Such a feat surprised the Saudi regime, which still hoped to maintain the earlier status quo with the help of the UAE and Bahrain (Kamrava, 2009: 403). Consequently, an attempted coup against Qatar was foiled in February 1996, and it is believed that Saudi Arabia provided support for this covert action (BBC News, 2000). This incident severely affected the future of Saudi-Qatari relations (Roberts, 2012).

During the next two decades, a veiled political and diplomatic contest took place between Doha and Riyadh, and tensions emerged in between occasional moments of entente (Al Qassemi, 2011; Gause, 2002; Kechichian, 2008). The geopolitical rivalry between Saudi Arabia and Iran is undoubtedly very salient in explaining the Saudis' mounting uncertainties concerning their regional sphere of influence. Since the 1979 revolution in Tehran, the Gulf region has been under immense pressure to contain the Islamic Republic's revolutionary fervour and aggressive foreign policy orientation. This is grounded in a "transnational Islamist model that [Iran] claims should apply throughout the region, although its strongest appeal is to fellow Shi'a" (Gause, 2017: 673).

The region's balance of power has been slowly but surely tilting in Iran's favour. After the U.S. toppling of Saddam Hussein in Iraq, the Baath regime was replaced by pro-Iranian forces. The rise of other Iranian proxies in countries like Lebanon, Yemen, and Syria, has pushed Saudi Arabia and Iran into a bitter cold war with a zero-sum game at play. This led to a continuous contest for influence among the domestic political systems of the region's small states (Gause, 2014: 1). The tense political environment has been further complicated by these two regimes' religious and ideological competition, as both aspire to impose their brands of Islam on the Muslim world [3].

The relationship between Qatar and Iran has been irritating Riyadh for decades. Firstly, Qatar shares the world's largest gas field with Iran (a.k.a. North Dome in Qatar, South Pars in Iran), 38 per cent of which lies under Iran's territorial waters (Erdbrink, 2010). The two countries signed several agreements to develop their cooperation in the field of oil and gas, and worked with Russia to establish a 'gas troika', an OPEC-style grouping (Hafezi, 2008). As a result, the three countries control an estimated 50 per cent of the world's natural gas reserves. Collaboration in this strategic area makes it highly unlikely that Doha will join any Saudi-led plans to contain Tehran economically. Conversely, Riyadh "seeks the shrinking, even the collapse, of the Iranian economy under sanctions" (al-Rasheed, 2018).

This high level troika arrangement also explains why Qatar kept diplomatic relations with the Islamic Republic amidst growing tensions between the Saudis and Iranians. For instance, Doha recalled its ambassador to Tehran in 2016 in protest over the ransacking of the Saudi missions in Iran by demonstrators angry at Riyadh's execution of a prominent Shiite cleric. Yet Qatar did not sever diplomatic ties with the Islamic republic, in contrast to Saudi Arabia and Bahrain who have broken off diplomatic ties with Iran since then (Finn, 2016b). The energy factor provides likewise an explanation for Qatar's backing of Turkish efforts, during 2010, to diplomatically resolve the dispute

over Iran's nuclear programme (Khaleej Times, 2010). Against this, the Saudis were manoeuvring behind-the-scenes for the U.S. to attack Iran and destroy its nuclear programme (Black and Tisdall, 2010).

Furthermore, the Saudi leadership aspires to have a say in the natural gas sector, especially after the drop in oil prices since 2014. International agreements (e.g. the 2015 climate conference in Paris) are paving the way for economies to suppress petrol and diesel-driven vehicles in the long run, given the cost-efficiency of renewable energies (Paltsev, 2016). These trends accelerate the decline of oil and conversely highlight the importance of natural gas, which is the cleanest fossil fuel. In fact, there are on-going initiatives that aim to increase the share of natural gas in the global energy mix (2016: 392). According to academic James Dorsey, "Saudi Arabia's problem is that Iran and Qatar have the gas reserves it does not. That is one reason why renewables figure prominently in Saudi Crown Prince Mohammed bin Salman's Vision 2030 reform program, not only to prepare Saudi Arabia economically for a post-oil future but also to secure its continued geopolitical significance" (Dorsey, 2018).

The quest for more international visibility and relevance has been at the core of Doha's endeavours too. Since 1996, the country has continuously strived to enhance its diplomatic status by playing the role of mediator and negotiator in several hot spots, including Ethiopia, Iraq, Israel and the occupied territories, Lebanon, Sudan, Yemen and Afghanistan (Hounshell, 2012). This created an image of Qatar as a "pygmy with the punch of a giant" (the Economist, 2011), but has also accentuated the country's risk appetite (Cooper & Momani, 2011: 114). In this process, Doha knitted a web of relations with different factions, including with pro-Iranian forces such as the Houthis in Yemen, Hezbollah in Lebanon, and activists in Bahrain.

The Saudis saw Qatar's active diplomacy in areas such as Yemen, Lebanon and Bahrain as a direct incursion. Subsequently, Saudi Arabia refused to attend some summits held in Doha, notably the one on Gaza, which was held in January 2009 and attended by Iranian President Mahmoud Ahmadinejad and Hamas political leader Khaled Meshaal (Black, 2009). At that time, Saudi Arabia was leading the so-called 'axis of moderation'— a de facto alliance including Egypt, Jordan, and the UAE. They stood closer to Israel's positions and in opposition to the so-called 'axis of resistance'— which included Iran, Syria, Lebanon, and some Palestinian movements (ACPRS, 2014: 1-2).

The other primary source of friction between Riyadh and Doha is not directly related to the Saudi-Iranian battle for influence. In its aspiration to impose leadership over the Sunni Muslim States, Saudi Arabia opposes the Muslim Brotherhood's political rise within several Arab countries. Doha has considerable influence over this transnational group (Gause, 2014: 3). However, this was developed for purely pragmatic and strategic reasons; "to maintain a proactive, ahead-of-the-curve approach to the region, Doha invested in good relations with non-state actors across the Arab world's political spectrum that Qatari decision-makers believed would shape the region's future for better or for worse" (Cafiero, 2017).

From a Qatari vantage point, the Arab uprisings, which started in Tunisia on 18 December 2010 and spilt over to other Arab countries, were an opportunity to shift the Middle East balance of power away from Saudi Arabia. These events allowed Doha to capitalise on two long term strategic orientations, weaving a web of influence with the Muslim Brotherhood, and building a mighty media empire (e.g. Al Jazeera). This strategy seemed to bear fruit as many Qatar-backed movements were about to attain power (albeit briefly as with the Muslim Brotherhood in Egypt).

Conversely, the Arab uprisings rang alarm bells for the Saudis and UAE. Both were vehemently opposed to any prospect of regime change and thus joined forces to impede the Arab Spring at all

costs. Initially, though, the Saudi / UAE axis half-heartedly supported the uprisings in Libya and Syria for tactical reasons (ACPRS, 2014: 2). So, while the Saudi / UAE axis and Qatar were in agreement over Bahrain, Libya, and Syria, they remained at odds over Tunisia, Egypt, and Yemen. Disagreement over the preferred course of action in the latter countries proved too hard to reconcile, and thus the relationship between the two sides reached its lowest ebb.

The Saudi/UAE axis offered arms and financial support to their counter-revolutionary proxies. In this context, they bankrolled the coup in Egypt, provided considerable military assistance to Libyan militia leader Khalifa Haftar, and gave substantial financial means to different political forces to prevent Tunisia's Ennahda from winning national elections (ACRPS, 2014: 3; Cafiero, 2017). Such meddling changed the uprisings from peaceful demonstrations to civil and sectarian wars. Meanwhile, Qatar continued its political relations with the Muslim Brotherhood, and offered some of its affiliates a safe haven, especially after the coup against the first democratically elected president in Egypt in 2013. Al Jazeera also maintained its pro-Arab Spring editorial line, deconstructing the counter-revolutionary narrative at every turn. Subsequently, Saudi Arabia, the UAE, and Bahrain withdrew their ambassadors from Qatar in early 2014 (Kirkpatrick, 2014; ACPRS, 2014). Nevertheless, discussions took place over the following months, and Qatar adopted a set of de-escalating measures. Relations among the Gulf Cooperation Council (GCC) countries appeared to be warming a few months later, as the three above-mentioned countries agreed in November 2014 to return their ambassadors to Qatar, signalling an end to an eight-month rift.

Cyber conflict in the Gulf 2010-2017

In parallel with the strategic and geopolitical upheavals in the region, a surge of cyber threats has also been observed. In a piece published by the *New York Times* in January 2010, more details emerged about the "Stuxnet worm" that had targeted Iran (Falkenrath, 2010). This malware is believed to have been developed by U.S. and Israeli covert operatives (Nakashima and Warrick, 2012), and was initially designed to infect the industrial-control systems of factories, electric power grids, refineries, pipelines, and industrial equipment. In particular, Stuxnet was unleashed to degrade the technology used in Tehran's nuclear facilities. The worm is said to have gained initial access via Microsoft Windows to a management system called "supervisory control and data acquisition" (The Economist, 2010b).

Some sources claimed that the attack destroyed about 5,084 out of 8,856 centrifuges in use at the Iranian nuclear facilities, and consequently, the Bushehr plant has been forced to shut down at least twice (Fleming, 2010). Iran, however, downplayed the impact of the attack. Tehran denied that any significant damage was done but admitted that some computers at its nuclear plant were compromised (The Economist, 2010a). Nonetheless, Symantec, a computer-security firm, stated that 60% of the computers infected with Stuxnet worldwide were in Iran; a rather considerable percentage which indicates there was more damage than officially acknowledged (The Economist b, 2010). Additional cyber strikes continued to hit Iran. For example, the Stars virus targeted governmental computer systems and was disguised within legitimate document types to deceive unsuspecting users into running them using official computers (Rashid, 2011). A third wave of attacks involved spyware named the Duqu Trojan, which was designed to steal data in order to help launch further cyber attacks (BBC News, 2011).

It has been asserted that Israeli intelligence operatives were behind these attacks. An article by the *New York Times* revealed the existence of Unit 8200, Israel's equivalent of America's National

Security Agency. This entity is thought to be behind some of the most sophisticated forms of modern cyber warfare. For instance, in 2007 they used complex jamming technologies to blind a Syrian radar installation before raiding a nuclear reactor under construction. A specialised industry publication, IEEE Spectrum, mentioned the possibility that a built-in kill switch was utilised to shut down the radar (Markoff, 2010).

However, Iran has not been solely on the receiving end. It is worth mentioning that the Islamic Republic organized its first national cyber defence exercise in October 2012. The Basij, a civilian paramilitary organization that operates under the Islamic Revolutionary Guards Corps (IRGC), stated that it was operating a "cyber army" with thousands of hackers recruited from universities and religious schools (Lewis, 2014: 3). Thus, Iranian operatives are believed to have instigated many attacks of their own. For instance, Saudi Arabia's national oil company (Aramco) was targeted in August 2012, and a computer virus known as Shamoon damaged 30,000 computers. Some experts believe that this cyber offensive was intended to stop energy production at the largest OPEC oil exporter. Other viewpoints consider that the trigger for this incident was most likely an earlier cyber attack on Iran's major oil terminal at Kharg Island (2014: 3).

In any case, Saudi officials said that the group behind it was highly organised across locations in four continents (Reuters, 2012). The digital blitzkrieg against Aramco was so severe that former U.S. Defence Secretary Leon Panetta said it was probably the most destructive cyber attack on a private business (Perlroth, 2012). The hackers claimed allegiance to a group named Cutting Sword of Justice and issued a statement in which they blamed Saudi Arabia for crimes and atrocities in several countries, including Syria and Bahrain (Reuters, 2012).

The Shamoon malware made a comeback in 2016 with a new wave of attacks against Saudi targets. This operation was very well planned, as the disk-wiping malware was configured with passwords that seem to have been stolen from the targeted organisations. The cyber raid was timed to occur at the start of the weekend so as to reduce the likelihood of discovery before maximum harm could be inflicted (Symantec, 2016). Several companies, which are linked to Aramco and located in the hub of the Saudi petrochemicals industry, experienced network disruption and tried to prevent the malware from spreading by shutting down their networks.

Furthermore, several incidents took place in Qatar during that period too. For example, in August 2012 Qatar's natural gas company, known as RasGas, was hit with a virus that shut down its website and email servers. The malware, however, did not affect the company's critical digital infrastructure that controls natural gas production and delivery (Zetter, 2012). In 2016, a more damaging attack targeted Qatar National Bank (QNB), one of the largest in the Middle East. Hackers managed to steal a massive amount of data including about 465,437 QNB accounts and published them online. The leaked information contained personal and contact details, but only a fraction of this compromised data included full account details (Finn, 2016a). The QNB hack seemed to have been conducted for political motives (arguably by state actors). The hackers appeared to know what they were searching for, and the data was labelled correctly. For instance, a folder was labelled SPY, Intelligence, and reportedly contained information about agents stationed in Qatar, ranging from MI6 to American, French, and Polish intelligence staff. Other folders had labels for Al Thani (the name of Qatar's royal family), Qatar's State Security Bureau, Ministry of Defence, and Al Jazeera (Gulf News, 2016).

The UAE experienced comparable levels of cyber threats. The *Gulf News* cited a report issued by cyber security firm Kaspersky, which listed the UAE as the 19th most vulnerable country in the world (Qatar ranked 10th) (Gulf News, 2015). The same report indicated that about 33 per cent of Kaspersky product users in the UAE were targeted in 2015, which places the UAE as a 'high risk' country for

electronic infections (D'Mello, 2016). Another report put forward by the Norton cyber-security firm estimated that about 200,000 residents of the UAE believe that their personal information was compromised online (D'Mello, 2016). Also, it was reported that the UAE is the subject of 5 per cent of all cyber attacks taking place worldwide and that such attacks have increased by 500 per cent in the period stretching from 2011 to 2016 (Altaher, 2016).

The Abu Dhabi government seemed aware of these risks. For example, a cyber command centre was set up in 2014 within the army's headquarters in order to confront cyber-threats (Thomas, 2014). Dubai has also established its Centre for E-Security to fight cyber-crimes (Sambidge, 2014). However, critics have highlighted that the UAE's cyber-security policy is connected with infringements against the civil liberties of political opponents, human rights activists, and journalists (Donaghy, 2016). The *New York Times* reported that the UAE authorities have allegedly spent vast sums on malware that is designed for domestic espionage. The report details how Ahmed Mansoor, a human rights activist, was jailed and fired from his job. Furthermore, his passport was confiscated, his car stolen, his email hacked, his location tracked, and his bank account robbed of $140,000. With the help of experts, Mansoor learned later that he was being monitored via governmental spyware installed on his devices (Perlroth, 2016). Other reports suggest that the UAE's mass surveillance system was established with the help of an Israeli company (Donaghy, 2016).

It is clear though that the cyber-security issues faced by the Gulf countries during this period reflected the strategic patterns of the region's international relations. Most of these incidents unfolded against a backdrop of on-going geopolitical rivalries between the Saudis and Iranians, aggressive competition among Gulf neighbours, and a clampdown on dissent within domestic public spheres.

Intensifications of cyber conflict May 2017 – May 2018

Developments in Gulf international politics spiralled out of control in the spring of 2017. The subsequent hostile actions directed at Qatar by the quartet were unprecedented. While I am sympathetic in principle to the Qatari position in this crisis because of the quartet's breach of international law, I am not uncritical of the Qatari stance, and my interpretations of the different measures undertaken do not mirror Doha's official position. In fact, I have critiqued Doha's foreign policy shift in the past. Back in 2014, I wrote: "Since 2011, Qatar's leadership has changed its foreign policy outlook from that of a mediator relying on soft power to that of an active player prepared to use hard power across the political landscape of the Middle East and North Africa…Yet, Qatar cannot sustain such a position." The article warned of the consequences yet to come (Cherkaoui, 2014: 28).

It is one thing to predict an escalation in the region, but another to forecast its scale and ramifications. There is no doubt that the scope of the tensions observed in the Gulf during May-June 2017 caught even the most seasoned observers by surprise. The crisis proper began unofficially on the evening of 19 April 2017, when unidentified hackers located a cyber-bug in the website of Qatar News Agency (QNA), exploited a vulnerability in its internal network code, gained full control of its entire network, and began mining data and text. However, the official start for the crisis occurred when hackers took over QNA's system (including social media sites) on 23 May at 11:45 p.m. and posted incendiary false quotes attributed to Qatar's Emir during his visit to a military graduation ceremony (Salisbury, 2017). The alleged speech was said to have praised Iran as an Islamic power and Hezbollah and Hamas as resistance movements while criticising the United States.

These purported opinions contrasted with the official stance of the President of the United States, Donald Trump, who had just advocated a hard-line stance on Iran during his Saudi visit a weekend

earlier. From a Saudi perspective, the previous meeting of the Saudi Crown Prince Mohamed Bin Salman with President Trump "was an important event in international relations, not only because it restored Saudi-American relations, but because it enforced the alliance between the two countries and thus restored power to the international system." With the view of confronting Iran, this meeting effectively ended the legacy of non-intervention adopted by the previous Obama administration (AlMuhaini, 2018).

Even though the hacking happened just before midnight on 23 May 2017, and despite the late and abrupt occurrence of this incident, guests were already present in the studio sets of Saudi-owned *Al Arabiya* news channel, and *Sky News Arabia* (the ruling family of Abu Dhabi own 50% of the latter). In the studios, commentators criticised Qatar as a major troublemaker in the region and mostly offered an aggressive interpretation of events. *Sky News Arabia* even went to the extent of claiming ownership of a video proving the Emir's remarks. The channel ended up providing visuals of the Emir at the military graduation but did not broadcast his speech. A voiceover comment described what he is purported to have said (Sky News Arabia, 2017).

Moreover, despite denials from Qatar's Government Communications Office (which said the stories were untrue), the Saudi and UAE media rejected the hacking story, and denounced Qatar for its alleged support for terrorism without providing much evidence. It is also worth noting that the quartet's networks did not ask a single Qatari political analyst to comment on the allegations (*The New Arab*, 2017a). When Al-Arabiya contacted Saudi academic Khaled M. Batarfi for comment, the phone line was cut as soon as the latter mentioned Qatar's official refutation of the on-going claims (Suleiman, 2017). Acting in unison, Saudi-owned newspapers, such as Asharq Al Awsat, Al Hayat, Al Eqtisadiah, Okaz and Saudi Gazette offered very critical commentary.

At the same time, the UAE and Bahrain authorities warned their citizens against expressing sympathy with Qatar on social media, and imposed lengthy jail terms for those who disobeyed. In Bahrain, anyone showing "sympathy or favouritism" to Qatar or objecting in any way to Bahrain's anti-Qatar policies became punishable by imprisonment of up to five years and a fine. Similarly, the UAE introduced a possible 15-year jail penalty for anyone criticising the government or expressing sympathy toward Qatar, "whether it be through the means of social media, or any type of written, visual or verbal form" (DeYoung, 2017). Likewise, local media outlet *Okaz* reported that the Saudi government had imposed punishment measures, according to which citizens would be sentenced to up to five years of jail time for showing sympathy to Qatar via social media [4].

These tensions quickly escalated and the quartet decided to establish a blockade against Qatar in July 2017. Consequently, diplomatic ties with Doha were severed. The only land route linking Qatar to the Arabian Peninsula was cut, while airspace passage over the four countries was also denied, forcing flights to travel by lengthier routes. This led to the disruption of existing supply chains and the immediate halt of food supplies during the month of Ramadan (more than 90 per cent of Qatar's goods used to come from Saudi Arabia via road). As a result, the cost of some imported food and medicine went up ten-fold (Gorvett, 2018). Moreover, Qatar's imports slumped dramatically during July and August, and investors began moving their money out of the country. Qatari nationals were also declared persona non grata in the quartet countries, and nationals from the quartet countries living in Qatar were ordered by their respective governments to quit Qatar or face severe penalties (Falk, 2018:3). In the assessment of Qatar's National Human Rights Committee (QNHRC), these measures amounted to a flagrant violation of international law (QNHRC, 2017: 5).

Shortly afterwards, the quartet issued an ultimatum of 13 demands to be met within ten days (McLean, El Gamal, and Finn, 2017). The list included closing the Al Jazeera and a dozen other

media outlets funded by Qatar directly or indirectly, severing ties with Iran and organisations such as Hamas, shutting down a Turkish military base, paying undetermined sums of reparations, and being subjected to monthly external audits (Middle East Eye, 2017). Several experts believe that these demands were designed to be rejected (Falk, 2018; Law, 2017; Ulrichsen, 2017). Meanwhile, the threat of military action was looming over Doha. These rumours were confirmed months later, when Qatar's defence minister stated in an interview with the Washington Post that the quartet intended to intervene militarily at the beginning of the crisis (Weymouth, 2018).

The fact that the quartet - with the same players - organised a foiled coup to overthrow the Qatari government two decades earlier (Kamrava, 2009: 403), in 1996, indicate that attempts to destabilise Qatar had occurred before Al Jazeera became a key media player, and prior to Hamas gaining control over Gaza, or Turkey establishing bases in Doha. Knowledge of this historical background raises questions vis-à-vis the quartet's rhetoric. In fact, given Qatar's wealth, soft power, and active diplomacy, the quartet's most recent manoeuvres were interpreted as an attempt to "reduce Qatar to a Saudi client state" (Lieven, 2017).

The rise of "little Sparta"

The aforementioned developments cannot be fully grasped without a close analysis of the UAE's behaviour. In the past decade, the UAE has increased investment in its defence capabilities and adopted an aggressive foreign policy. For some, this militaristic drive earned the UAE the nickname of the Gulf's "little Sparta" (Chandrasekaran, 2014; Law, 2017; The Economist a 2017). Initially, retired General James Mattis, presently the U.S. Secretary of Defence, coined this moniker.

The UAE has primarily relied on Washington to build its military and intelligence apparatus and has managed to acquire an advanced air force, robust Special Forces, and serious cyber-warfare capabilities. The build-up was primarily financed by the country's wealth. The UAE and Qatar have many commonalities historically, geographically, culturally, and economically. They are both allied with the West and, generally, the United States. In particular, both states require foreign labour, and both depend largely on oil and gas as economic resources. Yet they were - and still are - opposed strategically and politically over several issues. The UAE is "one of the world's smaller countries, both territorially and demographically, but [it is] also among its wealthiest per capita. In possession of an estimated 8.1 per cent of the world's proven remaining petroleum reserves, it is the fourth largest international oil exporter" (Ibish, 2017: 3). Likewise, despite being a small state too, Qatar is also one of the world's wealthiest nations thanks to its ownership of the world's third-largest reserves of natural gas, which made it the world's largest liquid natural gas exporter (Champion, 2017).

However, as I will explain, the two countries were, and are, opposed strategically and politically over several issues. The UAE's militaristic drive has been described as enhancing Abu Dhabi's "outsize ambitions and regional clout" (Fahim and Ryan, 2017). Under the impetus of the Crown Prince Muhammad bin Zayed, the UAE adopted an aggressive and offensive posture, and "has gone from being a haven mindful of its own business into the Arab world's most interventionist regime. Flush with petrodollars, he has turned the tiny country, whose seven component emirates have a combined population of almost 10m (only about 1m of whom are citizens), into the world's third-largest importer of arms. He has recruited hundreds of mercenaries" (The Economist a, 2017).

One of the influencers behind this move is Erik Prince, the founder of one of the largest and most notorious mercenary armies in the world, namely Blackwater Worldwide. This was since rebranded as 'Xe Services', then reportedly sold as 'Academi' in 2011, before merging with its rival 'Triple

Canopy'. It is thought that these rebranding and business transactions were done after Prince faced countless legal challenges in the United States (Tran, 2014), which is why Blackwater's founder resettled in the UAE in 2010. He was then hired by the Crown Prince Muhammad bin Zayed to assemble a battalion of foreign private contractors for the U.A.E. They comprised various nationalities ranging from South African to Chilean and Colombian and were trained by veterans of the German and British Special Forces, the French Foreign Legion, and retired American officers.

According to Spanish daily *ABC*, which cites Qatari sources, the number of foreign mercenaries trained by Blackwater is estimated to be around 15,000 (De Andres, 2017). A *New York Times* article further elaborated on their mission, stating that "the force is intended to conduct special operations missions inside and outside [emphasis added] the country, defend oil pipelines and skyscrapers from terrorist attacks and put down internal revolts". The article cited documents to the effect that such troops could be deployed if the Emirates faced unrest in their crowded labour camps or were challenged by pro-democracy protests like those sweeping the Arab world (Mazetti and Hager, 2011).

Contrarily, Qatar pursued a different path. The authorities did not build a big army upon independence and did not spend heavily on weapons and equipment in comparison with other countries in the region. They also opted for different suppliers. For example, during the 1980s most of Qatar's arsenal was purchased from France. However, when Saddam Hussein's Iraq invaded Kuwait in the early 1990s, Qatari decision-makers sought closer military cooperation with the United States to confront ascending military threats in the region.

The relationship between Qatar and the United States only developed with the signing of the Defence Cooperation Agreement in June 1992 (renewed twice in 2002 and 2013). The latter became the lynchpin of a defence strategy whereby the Qatari leaders agreed to host an American presence, with the aim of boosting regional security. However, the US-Qatar agreement stopped short of being an all-encompassing defence pact, which would legally require the U.S. to intervene militarily on the side of Qatar should they come under armed attack. It is understood that the current agreement between both parties merely obliges the signatories to consult and/or cooperate in a military crisis (Saidy, 2017: 289). Needless to say, this became Doha's strategic Achilles' heel during the early phases of the current conflict, when the U.S. President appeared to be siding with the quartet.

Furthermore, the UAE built extensive cyber warfare capacities beyond conventional firepower. The Abu Dhabi authorities chose to work through a new and well-funded private company called DarkMatter. The latter claims to be a predominantly cyber-security firm, whose endeavour is to provide defensive measures against destructive cyber attacks. However, investigative journalist Jenna McLaughlin reported for *The Intercept* a story which debunks this narrative (Mclaughlin, 2016). She contended that despite claims to the contrary, the raison d'être of this organisation was to build the perfect surveillance state. Other reports gave credence to this perspective by highlighting that DarkMatter often recruited staffers with backgrounds in Western military and intelligence agencies, including the U.S. National Security Agency (NSA) (Cornwell, 2018). Additionally, 80 per cent of the firm's revenue derives from governmental contracts in the UAE, including - as many suspect - the local version of the NSA, namely the Signals Intelligence Agency (Gambrell, 2018). The use of a private sector company conceals the responsible agent and ensures plausible deniability if certain operations are exposed or fail to achieve the desired goal.

Concerning the Qatar News Agency (QNA) hack that triggered the current Gulf crisis, it is worth noting that the Qatari authorities promptly asked the United States for assistance. A unit from the Federal Bureau of Investigations (FBI) was subsequently dispatched to Qatar to conduct a comprehensive investigation. A couple of weeks later, Qatar's attorney general stated that the security

breach was initiated from countries laying siege to his country, and in a press conference held at Qatar's Ministry of Interior (MOI), Captain Othman Salem al-Hammoud, Assistant Director of MOI Information Security Department, thoroughly explained the sequence of events. He stated that "for 15 minutes, the [QNA] website experienced a surge in the number of visits - 41 visits - originating from the UAE in particular. The hike in the number of visits showed the hackers' eagerness to make sure that the planted news had been circulated" (Adly, 2017).

Correspondingly, the *Washington Post* published an article that corroborated the hacking story, sourcing its information back to U.S. intelligence officials. The article affirmed that "the United Arab Emirates orchestrated the hacking of Qatari government news and social media sites in order to post incendiary false quotes attributed to Qatar's emir in late May that sparked the on-going upheaval between Qatar and its neighbours" (Nakashima and DeYoung, 2017). The *Post* reported that "officials became aware last week that newly analysed information gathered by U.S. intelligence agencies confirmed that on May 23 [the day before the alleged hack took place], senior members of the UAE government discussed the plan and its implementation. The officials said it remains unclear whether the UAE carried out the hacks itself or contracted to have them done" (Nakashima and DeYoung, 2017).

The United Arab Emirates and the Russian perspective

Even though the UAE has been traditionally sourcing its military equipment and know-how from the U.S., a Russian blueprint seems to have directly inspired UAE cyber warfare capabilities and methods of operation. This probably happened because of the Russian cyber skills that were demonstrated in numerous theatres of war (e.g. the 2008 Russia-Georgia war, the Russia-Ukraine conflict). The cyber war against Georgia in 2008 is the first known cyber offensive that occurred simultaneously with land, sea, and air military operations, and is considered the best contemporary example of how to appropriately use computer network attacks in battle (Schreier, 2015: 112). The theory underpinning Russia's IW paradigm is straightforward. It sees such operations as a means to influence "the consciousness of the masses [...] by use of special means to control information resources as 'information weapons'" (Darczewska, 2014: 12). The Russian approach combines "the military and non-military order and the technological (cyberspace) and social order (information space) by definition" (2014: 12).

It is worth noting here that the Russian authorities also rely on a private contractor, namely the Internet Research Agency, to coordinate some of the Kremlin's digital influence operations (Seddon, 2014). This measure offers the safety of plausible deniability if needed. Also, almost every measure that Russia deployed during the annexation of Crimea and the conflict with Ukraine was duplicated in the UAE's hostile move against Qatar. The role of Russian sponsored television and agencies, such as Sputnik and RT (formerly known as Russia Today), in spreading disinformation concerning the conflict with Ukraine has been previously reported (Rutenberg, 2017). Moreover, the use of hackers in waging a relentless cyber war against Ukrainian state institutions has also been well documented (Paul and Matthews, 2016), while vicious cyber war operations have reportedly been targeting Ukraine's finance and defence ministries, as well as the state treasury that allocates cash to government institutions and other critical infrastructure (Zinets, 2016).

A study conducted by Christopher Paul and Miriam Matthews for the RAND Corporation concluded that there are four characteristics of modern Russian disinformation campaigns. Specifically, they are: "(1) voluminous and multi-channelled, (2) rapid, continuous and repetitive, (3)

noncommittal to objective reality, and (4) inconsistent in its messaging" (Paul and Matthews, 2016: 2). The research reveals how Russian propaganda is produced via text, video, audio, and photos, using multiple delivery platforms through the Internet, social media, satellite television, radio, and traditional television broadcasting. There is no doubt that without intensification and repetition, disinformation would have minimal impact. What makes Russian propaganda more damaging is the mix between mainstream media and the use of bots, cyborgs, and 'troll factories,' which - when combined - amplify the agent's messaging presence on social media. Such variety in delivery methods gives an aura of persuasiveness and confidence in the reliability of the arguments, particularly when it is coupled with a semblance of diversity that conveniently leads to the desired conclusions.

The second characteristic highlighted by the RAND study is that Russian info-warriors do not wait to corroborate whether the information conveyed is right or wrong - they tend to disseminate first and instantly begin interpreting events that seem favourable to their side. This gives them not only autonomy but also the capacity to stay ahead of the news cycle. This way they regularly offer breaking news, as well as non-news and non-events, and influence at times legitimate third-party news outlets. For example, when German news sources relayed Russian disinformation about atrocities in Ukraine in early 2014, echo-chamber systems used, relayed, and reprocessed the biased information. Other examples include the story alleging that Islamic State fighters were joining pro-Ukrainian forces (Paul and Matthews, 2016: 4). This non-commitment to truth is consistent with propaganda's classic mix of truth and falsehoods. As Professor Stanley Cunningham explains, "propaganda uses facts and poses as truthful information; it instrumentalises truth; it does falsify, but in ways that involve the use of truths and facts as much as possible" (Cunningham, 2002: 98).

The RAND study reveals several cases in which Russian info-warriors have been caught using paid actors to play the role of victims of alleged atrocities or crimes for news reports. Examples include the Viktoria Schmidt case (in Germany for Russia's Zvezda TV network, she claimed to have been the subject of aggressive behaviour from Syrian refugees). In another case, Maria Katasonova faked an in-house video with edited explosion sounds in the background, while claiming this was taking place on a battlefield in Donetsk. One observer has noted that "several scholars and journalists, including Edward Lucas, Luke Harding, and Don Jensen, have reported that books that they did not write—and containing views clearly contrary to their own—had been published in Russian under their names" (Paul and Matthews, 2016: 5).

Russian info-warriors do not seem to be too concerned with the consistency of their messaging, which indicates they have broad autonomy to broadcast different themes and messages, sometimes even relaying conflicting narratives. According to Maria Snegovaya, a doctoral candidate in political science at Columbia University, contemporary Russian propaganda follows the old Soviet legacy of the "4D approach: dismiss, distort, distract, and dismay" (cited in Wilson, 2015). Additionally, the RAND research estimates that such messaging disorder cascades directly from the behaviour of Russian President Vladimir Putin, who denied for example that Russian soldiers were involved in Crimea but later admitted that they were. Similarly, Putin disavowed any intention to annex Crimea, but then admitted that this was the plan all along (Paul and Matthews, 2016: 8).

It could be argued that many of Russian's modern propaganda tactics were replicated in the Gulf crisis. For instance, a few days before the hack on Qatar News Agency, active hashtags were setting the scene for what was coming. Academic and Gulf Affairs researcher Marc Owen Jones noted that there was an active Twitter hashtag linking Qatar with terrorism. Owen's analysis shows the presence of propaganda bots on numerous hashtags (bots are computer programs that work automatically). Owen wrote: "20 per cent of the Twitter accounts were anti-Qatar bots. Many of them were posting

well-produced images condemning Qatar's relations with Hamas, Iran and the Muslim Brotherhood. Other images shared in the Twitter campaign singled out Qatar's media channels as sources of misinformation. Almost all of the bot accounts tweeted support toward King Salman and Saudi's new relationship with Trump. During the Riyadh summit, these same bots posted thousands of tweets welcoming Trump to Saudi Arabia" (Jones, 2017).

The combination of highly organised smear campaigns on social media and satellite media networks also took place. Soon after the hacking, several Twitter hashtags were launched to mirror earlier accusations, such as the hashtag that trended in the UAE under the title #Qatarfundsterrorism. Another hashtag, "cutting ties with Qatar", became the number one trend worldwide with more than one million mentions at the time of publication (Al Jazeera, 2017a). Such unanticipated popularity underlines the use of bots to tweet and retweet the quartet's propaganda on a vast scale.

A comprehensive study conducted by the University of Oxford documented how info-warrior teams, which work for different governments around the world, run fake accounts to hide their traces. The researchers stated that "In many cases, these fake accounts are 'bots'—or bits of code designed to interact with and mimic human users" (Bradshaw and Howard, 2017: 9). These bots inundate social media platforms with fake news and unsolicited publicity, and are used to magnify insignificant opinions or players by inflating the number of likes, shares, and retweets. According to an earlier report issued by Freedom House in 2013, bots have frequently been deployed by Saudi Arabia. In fact, pro-government trolls and bots specialise in what the report describes as "hashtag poisoning", which is "a method of spamming a popular hashtag to disrupt criticism or other unwanted conversations through a flood of unrelated or opposing tweets" (Freedom House, 2013: 8).

During the crisis, it was common to see Saudi trolls on Twitter mocking the small size of Qatar. One of them threatened: "the Al-Suweidi neighbourhood [in Riyadh] is bigger than Qatar. It is just a matter of weeks and it [Qatar] will become a Saudi city" (Harding, 2017). Other tweets aimed to weaken the Qatari population's morale, as when a UAE hashtag "claimed the Emirates would snatch the 2022 football World Cup from Qatar #UAEwillhosttheWorldCup" (Harding, 2017). In the view of academic Khaled Hroub, professor of Middle East politics and Arab media at Northwestern University in Qatar, such a concerted campaign revealed that media in the region are now "an integral part of the 'war arsenal' of many states," adding that "official and semi-official media, mostly TV broadcasting and social media, along with encouraged 'national media volunteers' have been deployed in phases like battalions, clearly orchestrated and seemingly under a control-and-command structure at the highest level" (Harding, 2017).

Saudi Arabia and Qatar

In the meantime, anti-Qatar vitriol broadcasted via Saudi-owned satellite channels such as Al Arabiya and UAE-owned Sky News Arabia became the norm. Relaying Al Arabiya channel's diatribes, the network's own English website published dozens of propaganda pieces against Qatar. The following headlines underlining this propagandistic drive featured prominently in the Al Arabiya website in the first few days of the crisis: "Qatar following Iran's policy of interference in the region's crises" [5]; "How Qatar and Iran's hardliners are very much alike politically" [6]; "Hezbollah and Qatar – a story of forbidden love?" [7]; "Haftar accuses Qatar of supporting terrorism in Libya" [8]; "Analysts raise fears of U.S. base's proximity to Hamas in Qatar" [9]; "Qatari intelligence founder: 'Doha has lost its mind'" [10]; and "Who runs Qatar behind the scenes?" [11]. As a result, Al Arabiya News Channel lost its broadcasting licence with Ofcom in the United Kingdom after Qatar complained that it was

violating the code of impartiality and accuracy in news sourcing (Middle East Monitor, 2018). This is particularly telling, as Ofcom enjoys international respectability for high standards in maintaining broadcasting codes for programming to which all UK broadcasters must comply.

Actually, the aforementioned propagandistic messages were not unusual when one considers that Saudi royals own large sections of Arab media, and keep them firmly in line with the official Saudi policies. The list of media organisations that are wholly or partly owned by Saudi royals is exhaustive and includes: the Middle East Broadcasting Centre (MBC), which operates six television and two radio channels; Orbit Communication Corporation; Arab Radio and Television (ART), the Rotana Group (the most extensive entertainment media company in the Arab world), the Lebanese Broadcasting Corporation (LBC), the Lebanese channel Al Mustaqbal TV, the Lebanese newspapers *Al Nahar* and *Ad Diyar*, in addition to dozens of religious channels (Yaghi, 2017: 42).

The quartet's actions utilised multi-channelled platforms (print media, satellite channels, social media, etc.), repetitive propaganda that is rapid and continuous, and exemplified non-commitment to the truth. These characteristics reflect the Russian model. The final characteristic, namely the inconsistency of messaging, warrants additional elaboration. The Qatar-Israel relationship, for example, was the source of severe anti-Qatar criticism from the quartet's media. The use of this theme underlines the quartet's failure in associating Qatar with anti-Iran rhetoric as the latter did not seem to gain much traction in the wider Arab world. Moreover, the anti-Israel argument lacks consistency, given that Saudi Arabia, the UAE, and Egypt feature prominently in the so-called "Israel-Arab nations against terrorism". This phrase was coined by President Trump during a speech he delivered in Saudi Arabia in May 2017. The speech itself was described as "part of a larger drive to plant the United States firmly in the camp of Sunni Arab nations and Israel in their confrontation with Shiite-led Iran" (Baker and Shear, 2017).

Even so, the quartet's media exuded criticism and condemnation whenever Qatar held any event in which Israelis would participate. For instance, when an Israeli tennis player competed in the 2018 Qatar ExxonMobil Open (Israelis have been playing in this tournament since 2008), a leading UAE print and online media outlet, *The National*, published an article with the headline "the Israeli tennis player's presence in Qatar infuriates citizens" [12]. Similarly, when an Israeli youth handball team played in Qatar, *Arab News* - a Saudi media outlet - put forward a critical article [13].

While the preceding examples underscore some of the methods utilised by the quartet, these actions fell short of IW in the proper sense of the word. In my view, a full-fledged cyber war, as part of a wider IW conflict did not take place during the Gulf crisis. There have been many cyber skirmishes, so to speak, with acts of hacking, cyber espionage, and even Distributed Denial-of-Service (DDoS) attacks. However, we did not witness anything equivalent to the cyber war waged by Russia against Georgia in 2008. There were no significant attacks on critical infrastructure or attacks on radar and military installations. Yes, there have been countless conventional actions of disinformation among Gulf participants and their backers, and heated and relentless contests took place in the social media domain and via satellite networks (mainly from the Saudi/UAE side). However, these contests concerned the narrativisation and meaning of events, and cannot be counted as part of a grand IW design. In fact, these actions were mainly superimposed against a backdrop of more traditional diplomatic manoeuvring, as well as political and economic warfare.

Qatar's response

Doha has proved much more resilient than the quartet initially planned. The military alliance with Turkey, and the decisiveness shown by the Turkish leadership in the first days of the crisis by urgently sending new troops to Qatar, precluded the likelihood of a Saudi military attack. Also, Doha's strong financial reserves mitigated the immediate consequences of the siege. Uninterrupted gas exports from Qatar to clients outside the Gulf region were critical to resisting additional external financial pressures. Here, the newly opened Hamad Port provided vital access to seaborne commerce, and Qatar Airways' ability to fly over Iran en route to the main destinations worldwide has been extremely valuable. These were all critical factors contributing to the ineffectiveness of the blockade.

From a strategic communications perspective, Qatar's response was generally adequate. Doha's initial reflex was to adhere and operate within the international law framework. In this context, the Qatari National Human Rights Committee (QNHRC) was particularly vociferous from day one, emphasising the illegality of the blockade and organising a series of international events to spread awareness about it. Among these gatherings was the conference titled 'Freedom of expression: Facing up to the threat' (24-25 July 2017), which was organised in cooperation with the International Press Institute, and the International Federation of Journalists. More than 150 representatives from international civil society organisations, academia, and human rights bodies were invited to discuss issues that were triggered by the Gulf crisis, among which were the demands by the quartet to shut down Al Jazeera and other media outlets.

Additionally, QNHRC also put forward its case to the United Nations' Office of the High Commissioner for Human Rights (OHCHR). They issued a press statement as early as 14 June, urging "all the States involved to solve this dispute as quickly as possible through dialogue, to refrain from any actions that could affect the well-being, health, employment and integrity of their inhabitants, and to respect their obligations under international human rights law" (UN News, 2017). Later in November 2017, a delegation from OHCHR visited Qatar, where they met with some 20 governmental and civil society groups, as well as people who had been affected by the blockade. A subsequent report from OHCHR entitled 'on the impact of the Gulf crisis on human rights' was particularly damning for the quartet (OHCHR, 2017).

Furthermore, Qatar also filed a wide-ranging legal complaint at the World Trade Organisation (WTO) to challenge the blockade imposed by Egypt, Bahrain, Saudi Arabia and the UAE. By following the steps underlined in the WTO grievance process, Doha formally triggered the procedure for the quartet either to settle the complaint or face litigation at the WTO (Asian News International, 2017). Moreover, Qatar put forward a request to the International Civil Aviation Organization (ICAO), a UN body which regulates international air travel, to seek a "consensus-based solution" that addresses "current regional concerns" following the quartet's closure of its airspace to flights from Doha (The New Arab, 2017b).

Resorting to the international legal framework also meant that Doha had to deal with unresolved issues of its own making, chief among them its treatment of migrant workers. During this crisis, the Qatari authorities tackled this problem head on. After many years of criticism from human rights organisations, Qatar introduced several reforms which were positively received by leading organisations, such as Amnesty International and Human Rights Watch, even though they reserved their final judgement upon their successful implementation (HRW, 2018). Similarly, the International Labour Organization closed a case against Qatar over its treatment of migrant workers (BBC News, 2017).

The second facet of Qatar's response, which stems from the above-mentioned approach, was to try and claim the moral high ground. Qatar undertook no retaliatory measures against the citizens of the quartet countries, even if diplomatic norms would accommodate such measures. For instance, at the opening of the 46th ordinary session of the Advisory Council (14 November 2017), Qatar's Emir highlighted the illegality of the blockade, noting that the quartet failed to produce any evidence for their allegations. Although noting the quartet's non-interest in a negotiated settlement, he vowed to pursue a policy of self-restraint out of "keenness to maintain the fraternal relations among the Gulf peoples," and reiterated his call for a dialogue based on mutual respect for sovereignty and joint commitments (Gulf Times, 2017). A few months later, a spokesperson for Qatar's ministry of foreign affairs repeated the same principles, stating "Qatar did not direct the citizens of siege countries to leave its territory, noting that those who were employed before the crisis remained in their jobs even now." She also noted that the numbers of people receiving health services provided by the State to citizens of the siege countries residing in Qatar during the September-November period surpassed the 300,000 mark (Gulf Times, 2018a).

This course of action gave significant diplomatic, political, humanitarian, and public relations' advantages to Qatar. It also made the third strategic feature of Doha's communication response, namely the adoption of the victim frame, quite effective. According to Giorgio Cafiero, the CEO of Gulf State Analytics, a geopolitical risk consultancy based in Washington D.C., "despite its strenuous efforts, the quartet has failed to successfully sell its anti-Qatar narrative to the diplomatic and defence establishment in Washington, although President Donald Trump and other current and former officials have expressed varying degrees of support for the ATQ [anti-Qatar quartet]. He goes on to remark that "the Saudi/UAE-led blockade of Qatar has arguably given Doha a valuable tool in Washington that it lacked prior to June 5, 2017: the victimhood card" (Cafiero, 2018). Although U.S. officials have their own concerns about Qatari foreign policy and Doha's ties with certain Islamist actors, Cafiero concludes that "the establishment in Washington found the ATQ's blockade of Qatar to be too harsh, strategically flawed, and unjustified. As a geographically small country blockaded by its larger neighbours that shared Qatar's only land border, Doha gained sympathy as an 'underdog' from unexpected quarters. Qatar has used its ability to portray itself as the victim of the quartet's 'bullying' to garner support in the U.S. and other Western countries" (Cafiero, 2018).

Diplomatic frenzy was another major facet of Qatar's approach. Doha has manoeuvred to break its regional isolation and reinforce its political and diplomatic relations abroad. National investments in Europe were a good starting point, and the regime received diplomatic support from Europe in general, and Germany in particular. The Qatari leadership also reinforced its alliance with Turkey. There has been a defence cooperation agreement with Ankara since 2014, and Turkey opened its military base in Qatar in 2016. Ankara and Doha acted fast to cement this relationship strategically, politically, militarily and economically by signing many agreements and memoranda of understanding. Meanwhile, Qatar drifted closer to Iran's orbit and re-established full diplomatic relations with Iran, returning its ambassador in August 2017. As Hasan (2018) recounts, "the envoy was recalled to Doha in solidarity with Riyadh following the storming of the Saudi embassy in Tehran, but Iran was quick to condemn the Arab quartet's actions, provided Qatar with crucial food supplies and the two have since launched a joint chamber of commerce to facilitate greater interaction".

In another diplomatic offensive, Doha stepped up its relations with Russia in military, political, economic, trade, scientific and cultural areas. Subsequently, Qatar signed hefty contracts for the purchase of military hardware, including Russia's renowned S-400 air defence system (Stratfor,

2018). Qatar's Emir paid a visit to Russia, which boosted bilateral cooperation and revealed the importance of these ties for Qatar. The Russian Defence Minister also paid an official visit to Qatar, during which an agreement on military-technical cooperation was signed (Gulf Times, 2018b).

It is worth noting that Qatar's weapons procurement jumped significantly with the emergence of evident tensions within the Gulf. Arms imports increased by 245% between 2012 and 2016 (Salacanin, 2018: 2). The arsenals of Saudi Arabia and UAE (respectively the world's second largest and fourth largest arms importers) overshadow that of Qatar (the 20th world's largest arms importer) (SIPRI, 2018). The recent arms race has forced Qatar to increase its arms imports and sign several significant deals. After the blockade, arms procurement resumed frantically, even though the Qatari Armed Forces could not absorb all of the incoming weaponry systems in such a short timeframe (Mouchantaf, 2017). One commentator notes that "Doha has significantly increased its arsenal and purchased aircraft from the United States including a $12bn deal finalised in June 2017 to buy U.S. F-15 fighter jets. It also signed an $8 billion Typhoon-fighter-jet deal with the United Kingdom and Rafale fighter jets and armoured vehicles from France. Paris and Doha have also signed commercial contracts worth $14.1 billion" (Salacanin, 2018: 6).

The procurement of large military contracts from powerful states, while very costly financially, was rather ineffectual militarily (given the lack of manpower available in such a short timeframe to man the sophisticated weaponry systems). But for Qatar it did represent a strong political statement. According to Pieter Wezeman, a Senior Researcher with the Stockholm International Peace Research Institute's (SIPRI) Arms Transfers and Military Expenditure Programme, "recent Qatari arms deals are a classic demonstration of this. Especially by winning U.S approval to sell the Gulf country major weapon systems at the very start of the dispute with its neighbours, Qatar undermined Saudi / UAE claims that it was a hostile power and underlined U.S support, despite Trump's public statements against it" (Mouchantaf, 2017).

President Trump's initial support for the quartet arguably contributed to successes arising from Qatar's communications strategy. He has been a divisive figure outside his domestic constituency. Trump's anti-immigrant crusade, anti-Muslim bans, dangerous rhetoric on criminal justice, the racist designation of "shithole" countries (Dawsey, 2018), and the demonisation of refugees (Amnesty International USA, 2017) have undermined the U.S.'s world image. An opinion poll published in June 2017 revealed: " the sharp decline in how much global publics trust the U.S. president on the world stage [which] is especially pronounced among some of America's closest allies in Europe and Asia, as well as neighbouring Mexico and Canada" (Pew Research Centre, 2017). The fact that Trump is perceived internationally as a bully meant that his initial backing of Saudi Arabia played in favour of Qatar during the Gulf crisis.

Furthermore, Doha was fortunate to receive assistance from an entirely unexpected party: hacktivists. An obscure group with a Russian email address, namely Global Leaks, engineered an embarrassing moment for the UAE. The collective hacked into the Hotmail account of Yousef al-Otaiba, the UAE ambassador in Washington D.C., and obtained many communications that were exchanged with senior officials, think tanks, PR executives, and journalists. Global Leaks then gave these documents to *The Intercept*, an online investigative journalism publication (Grim, 2017). The emails revealed UAE lobbying efforts to shape a US foreign policy narrative biased against and detrimental to Qatar. It is hard to quantify the impact of these revelations, but they may well have played a role in undermining the UAE's arguments and credibility within Washington (Dorsey, 2017).

However, Qatar's communication strategy is far from being perfect. Doha has been the subject of media flak since 2014 over various matters (these include alleged relations with terrorist

organisations, migrant workers' welfare, and allegations surrounding the 2022 FIFA World Cup bid). The Qatari authorities were generally slow to react and merely offered sparse and defensive comments here and there. And while the UAE was building an extremely potent network among influential personalities in the U.S., Qatar relied on a traditional diplomacy track and omitted to establish a clear-cut strategic communications strategy that would have countered the disinformation campaigns from the very beginning. This would have limited the negative impact on the nation's brand and reputation.

Then, because it had to compensate for the time lost, Doha was not efficient at first in its use of lobbyists and public relations firms despite their massive spending in this area. The journalist Simon Henderson, who visited the Gulf region in September 2017, criticised the reliance of all sides on Washington DC's lobbying industry. Henderson observed that "the only winners so far are the lobby groups making good money by providing advice, devising strategies, and setting up opposition websites and conferences. Seldom has the term 'beltway bandits' seemed more appropriate" (Henderson, 2017). Ultimately though, Doha seemed to have navigated the murky waters of the Washington lobbies and got back into the political game in Washington D.C. after allocating even more resources to this end (Harris, 2018b).

Conclusion

Information Warfare increasingly influences the waging of war and thus creates new challenges for traditional military strategies, while opening up new opportunities to dominate adversaries. Among the novelties of the past decade is the addition of cyberspace as a theatre of war, standing equally alongside land, sea, air, and space. The extension of warfare to cyberspace has brought numerous advantages to the U.S. but has also enabled other nations like Russia to gain a competitive edge in an evolving field. In any case, as Russian war experiences in Georgia and the Ukraine have revealed, cyber attacks are now deployed hand in hand with other elements of IW, and in synergy with combat operations for the control of battle space, conflict space, and information space. Therefore, many armies are studying, if not emulating, the Russian IW blueprint (Bond, 2018).

The concerted actions of Egypt, Saudi Arabia, Bahrain and the UAE could have devastated Qatar. They had the offensive advantage, established the surprise effect, used private contractors to ensure plausible deniability, and directed cyber strikes against Qatar's information nodes, such as their news agency, while putting propagandistic messages in these locations. Likewise, Al Jazeera's website was subjected to a cyber attack in early June 2017, but the network's engineers managed to fend it off (Brandom, 2017). In the meantime, the quartet's strategists tried to impose censorship on Al Jazeera (Al Jazeera, 2017b) in the hope that the audiences would switch to other Gulf media outlets. In parallel, trolls and bots were employed to push the quartet's narrative in cyberspace. These media and cyber hostilities occurred against a backdrop of economic blockade and a total diplomatic offensive against Qatar.

Nevertheless, the Gulf crisis did not escalate to a full-fledged cyber war, and thus Information Warfare (in the proper sense of the word) did not take place. The relatively small-scale attacks that took place in the Gulf did not reach the level of the cyber war waged by Russia against Georgia in 2008. A key factor here is that Qatar's Al Udaid base houses the Qatari Air Force, U.S. Air Force, Royal Air Force, and other Western personnel and equipment. This means that any sustained cyber-attack on Qatar's assets would threaten U.S. operations as well. This explains why the Saudi/UAE axis did not commit themselves to an all-out cyber war. In fact, according to the axis narrative, their

goal from the onset was to isolate and discipline Qatar, not to wage war. Initiating an all-out cyber war would have changed the narrative of the conflict from a limited operation aiming to 'boycott' an irritating neighbour to an inter-state war, hence directly implicating the U.S.

One must also remember that the military option was removed from consideration after Turkey's decision to send military reinforcements in the first hours of the crisis. There were also frictions at the top echelon of the U.S. administration (Trump versus Tillerson and Mattis) (Tibon, 2018), which are believed to have put a halt to Saudi and UAE military movements alongside the Qatari borders. Taking hard power out of the equation played a big part in reducing the prospects of military conflict (including an all-out IW blitzkrieg).

Overall, the Gulf crisis illustrates the interplay between numerous historical, geopolitical, economic, strategic, and military factors. The Middle East region, including the Gulf, has an unpredictable and fluid pattern of alliances which have challenged even the most established theories of regional international relations (Gause, 2017: 672). Qatar has engaged in very active diplomacy in the past two decades and has therefore established itself as potent interlocutor for a myriad of political players, infuriating Riyadh in the process. At the same time, Doha has tried to balance its relations with both regional rivals Iran and Saudi Arabia.

This balancing act did not please Riyadh, which would like a more submissive neighbour next door. Besides, Doha's support of the Arab Spring inevitably collided with Riyadh's strategy. Meanwhile, a new leadership emerged in Saudi Arabia amidst the palace coup of April 2015, as Mohammed bin Salman jumped the succession line, and established himself as the upcoming king (Hearst, 2017). Unlike his old and lethargic royal uncles, the new leader is unpredictable. Western governmental agencies have previously voiced their concern that Riyadh was becoming impulsive in its foreign policy (Reuters, 2015).

The blockade has proven the usefulness of Doha's diplomatic network. Rather than falling into isolation, Doha has solidified its relations with regional powers - Turkey and, to a lesser extent, Iran. Qatar has also found good support from Oman and Kuwait, in addition to Morocco, Algeria and Tunisia, along with Asian governments. While it would have been entirely reasonable for a small state to retreat in front of such an alliance of larger powers, Qatar's resilience has intrigued its enemies, and has proven, in the words of international relations scholar Robert Jervis, that "relatively small and weak states can hold off larger and stronger ones, or can deter attack by raising the costs of conquest to an unacceptable level" (Jervis, 1978: 162, 190).

The quartet's plan appears to have relied on outdated information too. For example, they believed that Qatar relied solely on the road passage with Saudi Arabia even though the construction of a state-of-the-art port in early 2017 allowed the freight of all kinds of exports and imports. Then, believing that their initial moves had scared Doha, the quartet sent an unrealistic list of grievances, mystifying even the most experienced diplomats (Reuters, 2017). Conversely, Qatar tried to occupy the moral high ground, which lent both credibility and consistency to Doha's strategic communications strategy. The latter had shortcomings too, but given the quartet's own inconsistencies, Doha's narrative tended to prevail (Hassan, 2018).

Within the Trump administration, hawks have taken the wheel on foreign policy and are pushing for yet another war, this time against Iran. Considering that the U.S. needs a unified front from its Gulf allies (Harris, 2018a), the diplomatic situation between the quartet and Qatar could gradually return to a semblance of normalcy. In the short-term and medium-term though, the foreign policy orientations of both sides remain on a collision course, unless a genuine and constructive strategic dialogue takes place (which is highly improbable at this stage). Nevertheless, all protagonists will

undoubtedly process the lessons learned from the most recent crisis. In a region that is already weakened by foreign interventions and rife with rivalries, the consequences of another major war will be devastating. Next time a full-fledged Information War is not to be discounted.

Endnotes

[1] For a review of the literature on IW and the Revolution in Military Affairs, see: J Arquilla (2007) Thinking about information strategy. In J Arquilla and DA Borer (Eds) *Information strategy and warfare.* New York: Routledge; C Bellamy (2001) What is Information Warfare? In R Matthews and J Treddenick (Eds) *Managing the revolution in military affairs*. New York: Palgrave; WA Owens and E Offley (2001) *Lifting the fog of war*. Baltimore: Johns Hopkins University Press; EA Cohen (1996) A revolution in warfare. *Foreign Affairs,* 37-54; EA Cohen (2001) Change and transformation in military affairs. *Journal of Strategic Studies* 27(3): 395-407; E Dahl (2002) Network centric warfare and operational art. *Defence Studies* 2/1(17); MJ Mazarr (1994) *The revolution in military affairs: A framework for defense planning*. Army War College. PA: Carlisle Barracks.

[2] For a review of the literature on Hacktivism, see: PA Taylor (2005) From hackers to hacktivists: Speed bumps on the global superhighway? *New Media Society,* 7(5): 625-646; G Coleman (2013) *Anonymous in context: The politics and power behind the mask*. Waterloo, CA: The Centre for International Governance Innovation; C Fuchs (2014) Anonymous: Hacktivism and contemporary politics. In D Trottier and C Fuchs (Eds) *Social Media, Politics and the State*, pp. 88-106. NY: Routledge; NCN Hampson, (2012) Hacktivism: A new breed of protest in a networked world. *Boston College International and Comparative Law Review,* 35(2): 511-542.

[3] It should be noted that Saudi Arabia has begun shifting since 2015 from the ideological dogma of Wahhabism to a new populist and militarised style of Saudi nationalism (al-Rasheed, 2018).

[4] https://www.elwatannews.com/news/details/2176402

[5] http://english.alarabiya.net/en/News/gulf/2017/05/31/DNP-Qatar-following-Iran-s-policy-of-interference-in-the-region-s-crises.html

[6] http://english.alarabiya.net/en/features/2017/05/29/ANALYSIS-How-Qatar-and-the-Khomeinis-are-very-much-alike-politically.html

[7] http://english.alarabiya.net/en/features/2017/05/27/Hezbollah-and-Qatar-a-story-of-forbidden-love-.html

[8] http://english.alarabiya.net/en/News/north-africa/2017/05/29/Haftar-accuses-Qatar-of-supporting-terrorism-in-Libya.html

[9] http://english.alarabiya.net/en/features/2017/05/29/nalysts-raise-fears-of-US-base-so-close-to-Hamas-in-Qatar.html

[10] http://english.alarabiya.net/en/features/2017/05/29/Qatari-intelligence-founder-Doha-has-lost-its-mind-.html

[11] http://english.alarabiya.net/en/views/news/middle-east/2017/05/26/Who-runs-Qatar-behind-the-scenes-.html

[12] https://www.thenational.ae/world/gcc/israeli-tennis-player-s-presence-in-qatar-infuriates-citizens-1.693420

[13] http://www.arabnews.com/node/1252056/sports

Author bio

Tarek Cherkaoui is Manager at the TRT World Research Centre (Turkey), and author of *The News Media at War: The Clash of Western and Arab Networks in the Middle East* (London: I. B. Tauris, 2017). Cherkaoui is an expert in the field of strategic communications analysis with a career that spans a range of industries, including the creative industries, not-for-profit, and higher education. He holds a PhD in media and communication studies from Auckland University of Technology. His research interests include the international broadcasting media, public diplomacy, soft power, information control, media-military relations, political and military affairs—specifically within a Middle Eastern context.

References

Abu Taleb H (2017) Qatar's political suicide. Available at: http://saudigazette.com.sa/article/179301/Qatars-political-suicide

ACRPS (2014) Recalling GCC ambassadors from Doha: A background and future predictions. *Arab Center for Research and Policy Studies*. Available at: https://www.dohainstitute.org/en/lists/ACRPS-PDFDocumentLibrary/Recalling_GCC_Ambassadors_from_Doha_A_Background_and_Future_Predictions.pdf

Adly A (2017) Qatar presents proof of UAE role in QNA website hacking. Available at: http://www.gulf-times.com/story/557315/Qatar-presents-proof-of-UAE-role-in-QNA-website-ha

Al Jazeera (2018) New details revealed on 1996 coup attempt against Qatar. Available at: https://www.aljazeera.com/news/2018/03/al-jazeera-reveals-details-1996-coup-attempt-qatar-180304200532130.html

Al Jazeera (2017a) Social media reacts to Gulf diplomatic rift. Available at: https://www.aljazeera.com/news/2017/06/social-media-reacts-gulf-diplomatic-rift-170605095334870.html

Al Jazeera (2017b) Saudi Arabia bans Al Jazeera channels in hotels. *TCA Regional News*, 9 June. Available at: http://www.aljazeera.com/news/2017/06/saudi-arabia-bans-al-jazeera-channels-hotels-170609141041079.html

AlMuhaini M (2018). The back story behind meeting of Mohammed bin Salman and Trump. Available at: https://tinyurl.com/y89tvj9q

Al Qassemi SS (2011) How Saudi Arabia and Qatar became friends again. Available at: http://foreignpolicy.com/2011/07/21/how-saudi-arabia-and-qatar-became-friends-again/

al-Rasheed M (2002) *A History of Saudi Arabia.* Cambridge University Press.

al-Rasheed M (2018) What fuels the Saudi rivalry with Iran? *The New York Times*, 23 April. Available at: https://www.nytimes.com/2018/04/23/opinion/international-world/saudi-iran-prince-mohammed.html

Altaher N (2016) UAE a target of 5 per cent of global cyber attack. *Gulf News*, 12 May. Available at: https://gulfnews.com/news/uae/crime/uae-a-target-of-5-per-cent-of-global-cyber-attacks-1.1826610

Amnesty International U (2017) *Trump's first hundred days.* Available at: https://www.amnestyusa.org/wp-content/uploads/2017/05/trump_first_hundred_days.pdf

Arquilla J (2007) Thinking about information strategy. In Arquilla J and Borer DA (Eds.) *Information Strategy and Warfare*. New York: Routledge, pp 1-15.

Asian News International (2017). Gulf crisis: Qatar makes legal complaint to WTO over trade boycott. *Asian News International,* 1 August.

BBC News (2000) Life sentences for Qatari coup plotters. Available at: http://news.bbc.co.uk/2/hi/middle_east/660887.stm

BBC News (2011) Iran says it has 'controlled' Duqu malware attack. Available at: http://www.bbc.com/news/technology-15721839

BBC News (2017) ILO drops Qatar migrant workers complaint after reforms. Available at: http://www.bbc.com/news/world-middle-east-41919692

Black I (2009) Gaza split prompts Arab countries to boycott emergency summit. *The Guardian.* Available at: https://www.theguardian.com/world/2009/jan/15/gaza-egypt-saudi-qatar-summit

Black I and Tisdall S (2010) Saudi Arabia urges US attack on Iran to stop nuclear programme. *The Guardian*, 28 November. Available at: https://www.theguardian.com/world/2010/nov/28/us-embassy-cables-saudis-iran

Blair BG (2001) *Strategic Command and Control*. Washington, DC: the Brookings Institution.

Bond D (2018) More countries are learning from Russia's cyber tactics. *The Financial Times*, 15 March. Available at: https://www.ft.com/content/b7dbc0de-1b04-11e8-aaca-4574d7dabfb6

Bradshaw S and Howard PN (2017) *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation.* Oxford: Oxford Internet Institute Working Paper. Available at: http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf

Brandom R (2017) Al Jazeera network hit with 'continual hacking attempts'. *The Verge*. Available at: https://www.theverge.com/2017/6/8/15763424/al-jazeera-continual-hacking-attempts-qatar-cybersecurity

Cafiero G (2017) Doha and Abu Dhabi's incompatible visions for the Arab world. Available at: https://lobelog.com/doha-and-abu-dhabis-incompatible-visions-for-the-arab-world/

Cafiero G (2018) Qatar's anti-bullying narrative. Available at: https://lobelog.com/qatars-anti-bullying-narrative/

CBS (2011) Julian Assange, the man behind Wikileaks. Available at: http://www.cbsnews.com/8301-18560_162-7286686.html

Chandrasekaran R (2014) In the UAE, the United States has a quiet, potent ally nicknamed 'Little Sparta'. *The Washington Post.* Available at: www.washingtonpost.com/world/national-security/in-the-uae-the-united-states-has-a-quiet-potent-ally-nicknamedlittle-sparta/2014/11/08/3fc6a50c-643a-11e4-836c-83bc4f26eb67_story.html

Cherkaoui T (2014) Al Jazeera's changing editorial perspectives and the Saudi-Qatari relationship. *The Political Economy of Communication* 2(1): 17–32.

Cornwell A (2018). Emerging Gulf state cyber security powerhouse growing rapidly in size. *Reuters.* Available at: https://www.reuters.com/article/us-emirates-cyber-darkmatter/emerging-gulf-state-cyber-security-powerhouse-growing-rapidly-in-size-revenue-idUSKBN1FL451

Cooper AF and Momani B (2011). Qatar and expanded contours of small state diplomacy. *International Spectator: Italian Journal of International Affairs* 46(3): 113–28

Cunningham SB (2002) *The Idea of Propaganda*. Westport, Conn.: Praeger.

Damjanovic DZ (2017) Types of information warfare and examples of malicious programs of information warfare. *Military Technical Courier* 65(4): 1044-1057

Darczewska J (2014) The anatomy of Russian information warfare. The Crimean operation, a case study. OSW Point of View, 42 (May). Available at: http://aei.pitt.edu/57173

Dawsey J (2018) Trump derides protections for immigrants from 'shithole' countries. *The Washington Post (Online)*, 11 January. Available at: https://search.proquest.com/docview/1986560191

De Andres F (2017) Mercenarios de blackwater se entrenaron para invadir qatar. Available at: http://www.abc.es/internacional/abci-mercenarios-blackwater-entrenaron-para-invadir-qatar-201710080136_noticia.html

Denning DE (1999) Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. Paper read at *The Internet and international systems: Information technology and American foreign policy decision-making*, 10 December, San Francisco, United States.

D'Mello S (2016) UAE major target for cyber criminals. *Khaleej Times*, 23 February. Available at: https://www.khaleejtimes.com/nation/general/uae-major-target-for-cyber-criminals

Department of Defense (2015a) The Department of Defense cyber strategy. Available at: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Department of Defense (2015b) Deputy Secretary of Defense Bob Work speech. The third U.S. offset strategy and its implications for partners and allies. https://www.defense.gov/News/Speeches/Speech-View/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies/

Department of Homeland Security. (2002). Homeland security act of 2002. Public Law 107-296, 107th Congress. Available at: http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf

DeYoung K (2017) Bahrain and UAE criminalize 'sympathy' for Qatar. *The Washington Post (Online),* 8 June. Available at: https://www.washingtonpost.com/world/national-security/bahrain-and-uae-criminalize-sympathy-for-qatar/2017/06/08/ce74a666-4c70-11e7-9669-250d0b15f83b_story.html

Donaghy R (2016) Secret UAE surveillance programme reveals the true face of a police state. *Middle East Eye*. Available at: http://www.middleeasteye.net/columns/secret-UAE-surveillance-program-reveals-police-state-595443598

Dorsey JM (2017) UAE Ambassador's hacked mails feed crucial policy debates. Available at: https://lobelog.com/uae-ambassadors-hacked-mails-feed-crucial-policy-debates/

Dorsey JM (2018) Natural gas: An underrated driver of Saudi hostility towards Iran and Qatar. Available at: https://moderndiplomacy.eu/2018/03/27/natural-gas-an-underrated-driver-of-saudi-hostility-towards-iran-and-qatar/

Energy Information Administration (2015) Qatar international energy data and analysis. Available at: https://www.eia.gov/beta/international/analysis_includes/countries_long/qatar/qatar.pdf

Erdbrink T (2010) Sanctions slow development of huge natural gas field in Iran. *The Washington Post*, 23 July. Available at: http://www.washingtonpost.com/wp-dyn/content/article/2010/07/22/AR2010072203933.html

Fahim K and Ryan M (2017). The UAE's hunt for its enemies is challenging its alliance with the United States. *The Washington Post*. Available at: www.washingtonpost.com/world/middle_east/uaes-drive-for-regional-influence-tests-its-military-alliance-withthe-united-states/2017/08/03/448683ee-6bd2-11e7-abbc-a53480672286_story.html

Falk R (2018) *A Normative Evaluation of the Gulf Crisis.* (HSF Policy Brief No. 1). New York: Available at: http://humsf.org/wp-content/uploads/2018/02/HSF_PolicyBrief_2.pdf

Falkenrath RA (2011) From bullets to megabytes. *The New York Times*. Available at: http://www.nytimes.com/2011/01/27/opinion/27falkenrath.html

Finn T (2016a). Qatar National Bank investigating alleged data hack. *Reuters*. Available at: https://www.reuters.com/article/us-qatar-ntl-bank/qatar-national-bank-investigating-alleged-data-hack-idUSKCN0XO22S

Finn T (2016b) Qatar recalls its ambassador to Iran after attacks on Saudi embassy. *Reuters*. Available at: http://www.businessinsider.com/qatar-recalls-its-ambassador-to-iran-after-attacks-on-saudi-embassy-2016-1

Fitri N (2011) Democracy discourses through the Internet communication: Understanding the hacktivism for the global changing. *Online Journal of Communication and Media Technologies* 1(2): 1-20.

Fleming R (2010) Bits before bombs: How Stuxnet crippled Iran's nuclear dreams. *Digital trends*. Available at: https://www.digitaltrends.com/computing/bits-before-bombs-how-stuxnet-crippled-irans-nuclear-dreams/

Freedom House (2013) *Freedom on the net: Saudi Arabia*. Washington D.C.: Freedom House. Available at: https://freedomhouse.org/report/freedom-net/2013/saudi-arabia

Fuchs C (2013) The Anonymous Movement in the context of liberalism and socialism. *A Journal For and About Social Movements* 5(2): 345-376. Available at: http://fuchs.uti.at/wp-content/Interface.pdf (accessed 25 March 2018)

Gambrell J (2018a) U.A.E. cyber firm DarkMatter slowly steps out of the shadows. Available at: https://www.bloomberg.com/news/articles/2018-02-01/uae-cyber-firm-darkmatter-slowly-steps-out-of-the-shadows

Gause FG III (2002) The foreign policy of Saudi Arabia. In: Hinnebusch R and Ehteshami A (Eds) *The Foreign Policies of Middle East States*. Boulder: Lynne Rienner Publishers, pp. 193-208.

Gause FG III (2014) Beyond Sectarianism: The New Middle East Cold War. Doha, Qatar: Brookings Doha Centre Analysis Paper No. 11. Available at: https://www.brookings.edu/wp-content/uploads/2016/06/English-PDF-1.pdf

Gause FG III (2017) Ideologies, alignments, and underbalancing in the new Middle East cold war. *Political Science and Politics*, 50(3), pp. 672-675.

Gorvett J (2018) Qatar weathers the storm. *Asia Times*, 1 March. Available at: http://www.atimes.com/article/qatar-weathers-storm/

Gough SL (2003) *The Evolution of Strategic Influence*. Carlisle Barracks, Pennsylvania.

Grim R (2017) Diplomatic underground: The sordid double life of Washington's most powerful ambassador. Available at: https://theintercept.com/2017/08/30/uae-ambassador-yousef-al-otaiba-double-life-prostitutes-sex-work/

Gulf News (2016) QNB hacking: What we know so far. *Gulf News*, 2 May. Available at: https://gulfnews.com/business/sectors/banking/qnb-hacking-what-we-know-so-far-1.1816989

Gulf Times (2017) Qatar moving ahead irrespective of blockade: Emir. *Gulf Times*, 15 November. Available at: https://search.proquest.com/docview/1963621923

Gulf Times (2018a) Qatar not to retaliate against siege countries. *Gulf Times.* Available at: http://www.gulf-times.com/story/577721/Qatar-not-to-retaliate-against-siege-countries

Gulf Times (2018b) Russia-Qatar ties on fast track. *Gulf Times.* Available at: http://www.gulf-times.com/story/586515/Russia-Qatar-ties-on-fast-track

Hafezi P (2008) Russia, Iran, Qatar agree to form "big gas troika." *Reuters*. Available at: https://www.reuters.com/article/us-iran-gas-opec/russia-iran-qatar-agree-to-form-big-gas-troika-idUSTRE49K36H20081021

Hammond A (2014) Qatar's leadership transition: Like father, like son. Policy Brief 95. *European Council on Foreign Relations*. Available at: http://www.ecfr.eu/page/-/ECFR95_QATAR_BRIEF_AW.pdf

Harding D (2017). Qatar crisis turns hostile on social media. *AFP International Text Wire in English*, 13 June. Available at: http://news.abs-cbn.com/trending/06/13/17/qatar-crisis-turns-hostile-on-social-media

Harris G (2018a) Pompeo's message to Saudis? Enough is enough: Stop Qatar blockade. *The New York Times*, 28 April. Available at: https://www.nytimes.com/2018/04/28/world/middleeast/mike-pompeo-saudi-arabia-qatar-blockade.html

Harris G (2018b In charm offensive, Qatar pushes for a comeback in Washington. *The New York Times*, 9 February. Available at: https://www.nytimes.com/2018/02/09/us/politics/trump-qatar-lobbying-embargo.html

Hasan H (2018) The Qatar guide to surviving an economic boycott. *The Middle East Monitor*. Available at: https://www.middleeastmonitor.com/20180323-the-qatar-guide-to-surviving-an-economic-boycott/

Hassan H (2018) Qatar won the Saudi blockade. *Foreign Policy*. Available at: https://foreignpolicy.com/2018/06/04/qatar-won-the-saudi-blockade/

Hearst D (2017) Saudi palace coup: The sequel. *The Huffington Post*, 26 April. Available at: https://www.huffingtonpost.com/entry/saudi-palace-coup-the-sequel_us_5900874ae4b00acb75f18347

Henderson S (2017) A field trip to the front lines of the Qatar-Saudi cold war. *Foreign Policy*. Available at: http://foreignpolicy.com/2017/09/28/a-field-trip-to-the-front-lines-of-the-qatar-saudi-cold-war/

Hounshell B (2012) The Qatar bubble. *Foreign Policy* May–June. Available at: http://foreignpolicy.com/2012/04/23/the-qatar-bubble/

HRW (2018) Qatar: Year of crisis spurred rights reforms. *Targeted News Service*, 18 January. Available at: https://search.proquest.com/docview/1988946581

Ibish H (2017) *The UAE's Evolving National Security Strategy.* (Issue Paper number 4). Washington: The Arab Gulf States Institute in Washington (AGSIW). Available at: http://www.agsiw.org/wp-content/uploads/2017/04/UAE-Security_ONLINE.pdf

Jones M (2017) Hacking, bots and information wars in the Qatar spat. *The Washington Post*, 7 June. Available at: https://www.washingtonpost.com/news/monkey-cage/wp/2017/06/07/hacking-bots-and-information-wars-in-the-qatar-spat

Kamrava M (2009) Royal factionalism and political liberalization in Qatar. *The Middle East Journal, 63*(3): 401-420.

Kechichian J (2008) *Power and Succession in Arab Monarchies: A Reference Guide.* Boulder: Lynne Rienner.

Khaleej Times (2010) Turkey says Syria, Qatar back Iran plan. *Khaleej Times*, 9 May. Available at: https://www.khaleejtimes.com/article/20100509/ARTICLE/305099952/1016

Kirkpatrick DD (2014) 3 gulf countries pull ambassadors from Qatar over its support of Islamists. Available at: www.nytimes.com/2014/03/06/world/middleeast/3-persian-gulf-states-pull-ambassadors-from-qatar.html

Law B (2017a) The Gulf's 'little Sparta' has big military ambitions. Available at: www.middleeasteye.net/columns/gulf-s-little-sparta-has-big-military-ambitions-1331398998

Law B (2017b) Saudi Arabia and UAE: When bullies come a cropper. Available at: https://www.alaraby.co.uk/english/comment/2017/7/3/saudi-arabia-and-uae-when-bullies-come-a-cropper

Lewis JA (2014). Cybersecurity and Stability in the Gulf. Gulf Analysis Paper. Middle East Program. Center for Strategic and International Studies, January. Available at: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/140106_Lewis_GulfCybersecurity_Web_0.pdf

Lieberman J, Collins S and Carper T (2011) A gold standard in cyber-defense. *The Washington Post*, 7 July. Available at: https://www.washingtonpost.com/opinions/a-gold-standard-in-cyber-defense/2011/07/01/gIQAjsZk2H_story.html

Lieven A (2017) Will Qatar be reduced to a Saudi client state? Available at: https://www.prospectmagazine.co.uk/magazine/qatar-saudi-arabia-gulf-client-state

Lynch M (Ed) (2017) *The Qatar Crisis*. Washington D.C.: Project on Middle East Political Science (POMEPS). Available at: https://pomeps.org/wp-content/uploads/2017/10/POMEPS_GCC_Qatar-Crisis.pdf

MacAskill E (2010) Julian Assange like a hi-tech terrorist, says Joe Biden. *The Guardian,* 19 December. Available at: https://www.theguardian.com/media/2010/dec/19/assange-high-tech-terrorist-biden

Maclean W, El Gamal R and Finn T (2017) Arab states issue ultimatum to Qatar: Close Jazeera, curb ties with Iran. Available at: www.reuters.com/article/us-gulf-qatar-demands-idUSKBN19E0BB

Markoff J (2010) A silent attack, but not a subtle one. *The New York Times*, 27 September. A6. 209.

Mazzetti M and Hager EB (2011) Secret desert force set up by Blackwater's founder. Available at: http://www.nytimes.com/2011/05/15/world/middleeast/15prince.html

McCullagh D (2010) U.S. Army worried about Wikileaks in secret report, 15 March. Available at: https://www.cnet.com/news/u-s-army-worried-about-wikileaks-in-secret-report/ (accessed 21 February 2018).

Mclaughlin J (2016) Spies for hire: How the UAE is recruiting hackers to create the perfect surveillance state. Available at: https://theintercept.com/2016/10/24/darkmatter-united-arab-emirates-spies-for-hire/

Middle East Eye (2017) Qatar crisis: Saudi-led states list 13 demands to end blockade. Available at: www.middleeasteye.net/news/qatar-blockade-uae-setsdemands-end-crisis-1190365222

Middle East Monitor (2018) Qatar victory as Saudi's Al Arabiya surrenders UK broadcasting license. Available at https://www.middleeastmonitor.com/20180216-qatar-victory-as-saudis-al-arabiya-surrenders-uk-broadcasting-licence/

Miller D (2003) Information Dominance: The philosophy of total propaganda control? Available at: http://www.scoop.co.nz/stories/HL0312/S00216.htm

Mouchantaf C (2017) A huge military build-up is underway in Qatar. But who will man the systems? Available at: https://www.defensenews.com/global/mideast-africa/2017/12/15/a-huge-military-buildup-is-underway-in-qatar-but-who-will-man-the-systems/

Nakashima K and DeYoung E (2017) UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to US intelligence officials. *The Washington Post.* Available at: https://www.washingtonpost.com/world/national-security/uae-hacked-qatari-government-sites-sparking-regional-upheaval-according-to-us-intelligence-officials/2017/07/16/00c46e54-698f-11e7-8eb5-cbccc2e7bfbf_story.html

Nakashima K and Warrick J (2012) Stuxnet was work of U.S. and Israeli experts, officials say. *The Washington Post.* Available at: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

National Human Rights Committee (2017) *4th Report on the Human Rights Violations Resulting from the Blockade Imposed on Qatar.* Doha, Qatar.

New York Times (2017) Misguided attacks on Al Jazeera. *New York Times*, 21 June. Available at: https://search.proquest.com/docview/1911618977

Norris Pippa (2001) *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide, Communication, Society, and Politics*. Cambridge, New York: Cambridge University Press.

OHCHR (2017) *OHCHR Technical Mission to the State of Qatar 17-24 November 2017*. Geneva, Switzerland: Office of the High Commissioner for Human Rights. Available at: http://nhrc-qa.org/wp-content/uploads/2018/01/OHCHR-TM-REPORT-ENGLISH.pdf

Onley J (2009) *Britain and the Gulf Shaikhdoms, 1820–1971: The Politics of Protection.* (Occasional Paper No. 4). Qatar: Centre for International and Regional Studies at Georgetown University in Qatar.

Paltsev S (2016) The complicated geopolitics of renewable energy. *Bulletin of the Atomic Scientists, 72*(6), 390-395. Available at: http://www.tandfonline.com/doi/abs/10.1080/00963402.2016.1240476

Paul C and Matthews M (2016) *The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It.* Santa Monica, Calif.: Available at: https://www.rand.org/pubs/perspectives/PE198.html

Perlroth N (2012) In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. *The New York Times*, 24 October. Available at: https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

Perlroth N (2016). Governments turn to commercial spyware to intimidate dissidents. *The New York Times*, 16 November. Available at: http://www.nytimes.com/2016/05/30/technology/governments-turn-to-commercial-spyware-to-intimidate-dissidents.html

Pew Research Centre (2017) U.S. Image Suffers as Publics Around World Question Trump's Leadership. Available at: http://scholar.aci.info/view/14bd17773a1000e0009/15ce6dedb940001b8871afa

Pullela P (2017) Qatar says Arab states' demands 'made to be rejected', says open to talks. Available at: https://www.reuters.com/article/us-gulf-qatar/qatar-says-arab-states-demands-made-to-be-rejected-says-open-to-talks-idUSKBN19M3NS

Qatar National Bank (QNB) (2015) Qatar economic insight 2015. Available at www.slideshare.net/JoannesMongardini/qnb-group-qatar-economic-insight-2015

Rashid FY (2011) Iran claims Stars virus a second cyber-attack. eWeek. Available at: http://www.eweek.com/security/iran-claims-stars-virus-a-second-cyber-attack

Reuters (2012) Saudi Arabia says cyber attack aimed to disrupt oil, gas flow. *Reuters.* Available at: https://www.reuters.com/article/saudi-attack/saudi-arabia-says-cyber-attack-aimed-to-disrupt-oil-gas-flow-idUSL5E8N91UE20121209

Reuters (2015) German spy agency warns of Saudi shift to 'impulsive' policies. *Reuters*. Available at: https://www.reuters.com/article/us-saudi-germany-warning-idUSKBN0TL1O020151202

Reuters (2017) After pointed criticism, Tillerson urges gulf demands be sent to Qatar. *Reuters*. Available at: https://www.reuters.com/article/us-gulf-qatar-usa-tillerson/after-pointed-criticism-tillerson-urges-gulf-demands-be-sent-to-qatar-idUSKBN19C2KW

Roberts D B (2012) Examining Qatari-Saudi relations, 28 February. Available at http://thegulfblog.com/2012/02/28/examining-qatari-saudi-relations

Rutenberg J (2017) RT, sputnik and Russia's new theory of war. Available at: https://www.nytimes.com/2017/09/13/magazine/rt-sputnik-and-russias-new-theory-of-war.html

Saidy B (2017) Qatari-US Military Relations: Context, Evolution and Prospects. *Contemporary Arab Affairs,* 10(2), pp. 286-299.

Salacanin S (2018) *The Growing Arms Deals in the Gulf: Existential Need or Fear Politics?* Doha, Qatar: Available at: http://studies.aljazeera.net/mritems/Documents/2018/1/22/435b5cc4bb214fa6a634f76e2b5cd96e_100.pdf

Salisbury P (2017) The fake-news hack that nearly started a war this summer was designed for one man: Donald Trump. Available at: https://qz.com/1107023/the-inside-story-of-the-hack-that-nearly-started-another-middle-east-war/

Sambidge A (2014) Dubai sets up e-security centre to fight cyber criminals. *Arabian Business*. Available at: http://www.arabianbusiness.com/dubai-sets-up-e-security-centre-fight-cyber-criminals-553771.html

Schreier F (2015) On cyber warfare. *Geneva Center for the Democratic Control of Armed Forces Horizon 2015* Working Paper No. 7. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf

Seddon M (2014) Documents show how Russia's troll army hit America. Available at: https://www.buzzfeed.com/maxseddon/documents-show-how-russias-troll-army-hit-america

Serracino-Inglott P (2013) Is it OK to be an Anonymous? *Ethics and Global Politics* 6(4), pp.217-244.

SIPRI (2018) Asia and the Middle East lead rising trend in arms imports, US exports grow significantly, says SIPRI. Available at: https://www.sipri.org/news/press-release/2018/asia-and-middle-east-lead-rising-trend-arms-imports-us-exports-grow-significantly-says-sipri

Sky News Arabia (2017) Watch the speech of the emir of Qatar on state television (in Arabic). Available at: https://tinyurl.com/yb2bogu5

Stratfor (2018) Qatar: For Doha, the best defense is a good arms dealer. *Stratfor*. Available at: https://worldview.stratfor.com/article/qatar-doha-best-defense-good-arms-dealer

Suleiman H (2017) Abdullah bin Hamad al-Athbah: The awareness of gulf citizens has stopped the spread of fake news (in Arabic). Available at: https://tinyurl.com/y7gxctmy

Sutter JD (2010) The technical muscle behind WikiLeaks. *CNN*. Available at: http://edition.cnn.com/2010/TECH/innovation/07/26/how.wikileaks.works/index.html

Symantec (2016) Shamoon: Back from the dead and destructive as ever. *Symantec Official Blog*. Available at: https://www.symantec.com/connect/blogs/shamoon-back-dead-and-destructive-ever

Taylor PA (2005) From hackers to hacktivists: Speed bumps on the global superhighway? *New Media Society* 7(5): 625-646.

The Economist (2010a) The meaning of Stuxnet. *The Economist*, 397(8702): 14.

The Economist (2010b) A worm in the centrifuge. *The Economist*, 397(8702): 63-64.

The Economist (2011) Pygmy with the punch of a giant. *The Economist, 401(8758): 55-56.*

The Economist (2017). The Gulf's little Sparta: The United Arab Emirates. *The Economist*, 423(9035), 38.

The New Arab (2017a) Emirati, Saudi media slammed for propagating Qatar 'fake news'. Available at: https://www.alaraby.co.uk/english/blog/2017/5/24/emirati-saudi-media-slammed-for-propagating-qatar-fake-news

The New Arab (2017b) UN aviation agency to intervene in Qatar airspace blockade. Available at: https://www.alaraby.co.uk/english/news/2017/6/15/un-aviation-agency-to-intervene-in-qatar-airspace-blockade

Thomas B (2014) UAE military to set up cyber command. *Defense World*. Available at: http://www.defenseworld.net/news/11185/UAE_Military_To_Set_Up_Cyber_Command#.Wt26fy5uaos

Tibon A (2018) With Tillerson out, Qatar and Saudis left sweating on where Pompeo stands on Gulf crisis. *Haaretz*. Available at: https://www.haaretz.com/us-news/.premium-qatar-and-saudis-left-sweating-on-where-pompeo-stands-on-gulf-crisis-1.5909914

Tran M (2014) Blackwater considered itself above the law, US state department was warned. *The Guardian*. Available at: https://www.theguardian.com/world/2014/jun/30/blackwater-security-firm-above-law-us-state-department-killed-17-iraqis

Ulrichsen KC (2017) The Gulf's demands on Qatar look designed to be rejected. Available at: https://www.theatlantic.com/international/archive/2017/06/qatar-saudi-arabia-trump-mattis-gcc-uae/531474/

UN News (2017) UN rights chief urges dialogue among Qatar and countries involved in diplomatic dispute. Available at: https://news.un.org/en/story/2017/06/559462-un-rights-chief-urges-dialogue-among-qatar-and-countries-involved-diplomatic

U.S. Department of State (2013) *Country Reports on Terrorism 2012*. Available at: http://www.state.gov/documents/organization/210204.pdf

Vegh S (2003). Classifying forms of online activism: The case of cyberprotests against the World Bank. In McCaughey M and Ayers MD (Eds) *Cyberactivism: Online Activism in Theory and Practice.* New York: Routledge, pp 71-96.

Weymouth L (2018) Qatar to Saudi Arabia: Quit trying to overthrow our government. Available at: https://www.washingtonpost.com/outlook/qatar-to-saudi-arabia-quit-trying-to-overthrow-our-government/2018/02/02/05a1a848-0759-11e8-8777-2a059f168dd2_story.html

Wilson A (2015) Four types of Russian propaganda. *Aspen Review Central Europe,* April. Available at: https://www.aspen.review/article/2017/four-types-of-russian-propaganda/

Winters J and Giffin J (1997). *Issue paper: Information Dominance vs Information Superiority*, 1 April. http://www.iwar.org.uk/iwar/resources/info-dominance/issue-paper.htm

Wolfsfeld G (1997) *Media and Political Conflict: News from the Middle East*. Cambridge, U.K.: Cambridge University Press. Available at: http://catalog.hathitrust.org/Record/003167879

Wong WH and Brown PA (2013) E-bandits in global activism: WikiLeaks, Anonymous, and the politics of no one. *American Political Science Association* 11(4): 1015-1033. Available at: http://politics.utoronto.ca/wp-content/uploads/2013/12/wong-and-brown-2013.pdf (accessed 27 February 2018)

Yaghi M (2017) Media and sectarianism in the Middle East: Saudi hegemony over pan-Arab media. *International Journal of Media & Cultural Politics,* 13(1-2): 39-56. Available at: https://search.proquest.com/docview/1923319375

Zetter K (2012) Qatari gas company hit with virus in wave of attacks on energy companies. *Wired*. Available at: https://www.wired.com/2012/08/hack-attack-strikes-rasgas/

Zinets N (2016) Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar. Available at: https://www.reuters.com/article/us-ukraine-crisis-cyber/ukraine-hit-by-6500-hack-attacks-sees-russian-cyberwar-idUSKBN14I1QC