Cyberconflict, Online Political Jamming, and Hacking in the Gulf Cooperation Council

AHMED AL-RAWI
Simon Fraser University, Canada

This article offers insight into the role of hacking during the Qatar diplomatic crisis in 2017. I argue that the Middle East region has been witnessing an ongoing cyberconflict waged among different factions separated along regional rivalries, political alliances, and sectarian divisions. In relation to Qatar, systematic and well-calculated cyberoperations and hacking measures have been employed to pressure the Qatari government and influence its regional policies. Hackers, whether state-sponsored or not, intentionally created a diplomatic crisis in response to the perceived oppositional and unilateral policies carried out by the Qatari government in the region. The hacking incident led to other cyber-retaliations, and there is currently a cyberconflict between Qatar and a few other Arab states. I argue here that hacking is a form of online political jamming whose goal is to influence politics and/or change policies, and its communication impact flows either vertically (top-down or bottom-up) or horizontally.

Keywords: hackers, regional politics, Qatar, GCC, Gulf crisis, cyberconflict, online political jamming

Few academic studies address hacking in the Middle East despite its importance in directly and indirectly impacting geopolitical developments in the region and elsewhere (Powers & Jablonski, 2015). In the political context of the Qatari hacking crisis, the tension between some Gulf Cooperation Council (GCC) countries and the state of Qatar can be traced back to regional rivalries, jealousies, and competitions (Lenderking, Cammack, Shihabi, & Des Roches, 2017). The first and most important source of this tension is that Qatar has been known for a long time to support the Muslim Brotherhood and other Islamic conservative groups such as Hamas. The Muslim Brotherhood, in particular, are regarded as terrorists in Egypt, Saudi Arabia, and the United Arab Emirates (UAE). Qatar, for example, actively supported Muhammed Mursi's rule in Egypt before he was toppled by the military rule headed by Abdulfatah Elsisi. In addition, one of the leaders of the Muslim Brotherhood, Yussif Al-Qaradawi, lives in Qatar and became known for his Al Jazeera TV show *Shariah and Life*, which stopped airing in 2013, and his website, Islamonline.net. In 2003 and 2004, Qatar made a series of secret agreements with its Gulf neighbors "barring support for opposition and hostile groups in those nations, as well as in Egypt and Yemen" (Sciutto & Herb, 2017, para 1). Yet some GCC countries have accused Qatar of not complying with these agreements while siding with Iran and Hezbollah, the two Shiite adversaries of Saudi Arabia, Bahrain, and the UAE (Sciutto & Herb, 2017).

Ahmed Al-Rawi: aalrawi@sfu.ca
Date submitted: 2018-02-26

In other words, Qatar is regarded by a few Arab countries as a rogue nation due to its often oppositional or different stances that clash with their geopolitical interests (Hedges & Cafiero, 2017).

A second source of tension is the fact that Qatar runs the Al Jazeera channel, which has become a divisive issue since it was launched in 1996 (Al-Rawi, 2017). Hundreds of complaints by Arab countries have been filed, and several cases that have caused diplomatic tension in the region are attributed to the way Al Jazeera handles and covers sensitive topics and taboos (Al-Rawi, 2017). The channel's coverage is also partly responsible for the issue of the 2014 withdrawal of GCC ambassadors from Qatar ("Why Did the 3 GCC," 2014), and it is accused of biased coverage on many topics and countries during and after the Arab Spring events due to ideological or political differences (Al-Rawi, 2015). In addition to other demands, the countries forming the anti-Qatari alliance wanted the Al Jazeera channel to be indefinitely shut down.

Finally, a few minor factors that have led to diplomatic tension include the fact that Qatar paid around $1 billion in ransom in April 2017 to free Qatari hostages taken by a Shiite militia in Iraq despite opposition from other GCC countries (Solomon, 2017). This Iraqi militia has close connections with Iran and Hezbollah (Arango, 2017). Other issues that have enhanced the tension in the region include the UAE's failed effort to partly host the 2022 World Cup (Grim & Walsh, 2017), Qataris' refusal to buy $100 billion of the Saudi Aramco stocks if they would be introduced into the New York Stock Exchange ("The Accused Live in Arab Countries," 2017), and Jared Kushner's failed attempt in 2015 to obtain a $500 million loan from a Qatari emir, prompting him to pressure Trump to take a hard line against Qatar (Swisher & Grim, 2018). It is also known that Kushner enjoys a very good relationship with the Saudi crown prince, Mohammed Bin Salman, whom he has visited a few times (Zakheim, 2017).

Some Arab states—especially Saudi Arabia and the UAE—had experienced periods of tense diplomatic relations with Qatar long before the hacking attempt (Ulrichsen, 2017). For example, the Qatari government claimed that a series of 14 op-ed articles appeared in late April in some U.S. newspapers just before the hacking operation. All the articles attempted to implicate Qatar with supporting terrorist groups (Kirkpatrick & Frenkel, 2017). As explained later in more detail, the leaked e-mails of Yousef Al Otaiba, the UAE ambassador to the United States, showed that the UAE actually wanted to tank Qatar's economy by hitting its currency hard. The goal was to force Qatar to share the 2022 soccer World Cup by highlighting Qatar's alleged "dwindling cash reserves" that presumably would prevent it from building the required infrastructure (Grim & Walsh, 2017, para 51). The leaked e-mails also reveal some of the UAE's public relations efforts, including awarding about $20 million to the well-known U.S. think tank the Middle East Institute (Grim, 2017) to criticize Qatar. Other leaked documents provided by people sympathetic toward Qatar indicate that the former Al Jazeera journalist Mohamed Fahmy received $250,000 from Al Otaiba to cover the legal fees of suing the channel for $100 million due to its action before and after Fahmy was arrested and imprisoned by Egyptian authorities, allegedly for supporting the Muslim Brotherhood (Kirkpatrick, 2017). In brief, anti-Qatari sentiment in the GCC region and elsewhere in the Arab world had been growing long before the hacking incident.

Shortly after Donald Trump's visit to Saudi Arabia on May 20–21, 2017, former White House chief strategist Steve Bannon affirmed that the visit had led to the escalation of regional tension with Qatar ("Steve Bannon Says Trump's Saudi Visit," 2017), and Saudi Arabia as well as the UAE seemed to be waiting for the U.S. administration’s green light to politically and economically corner Qatar and pressure it. In fact, Saudi Arabia, the UAE, Bahrain, and Egypt—and later the Maldives, Mauritania, Yemen, and Libya as well—fully cut diplomatic and economic ties with Qatar on June 5, 2017. Saudi Arabia also announced that Qatari troops would no longer be part of the GCC unified army stationed in Yemen, while the UAE sent strong warnings to its citizens and residents to refrain from publicly sympathizing with Qatar. Some observers believe that the diplomatic tension reached a point where Saudi Arabia was planning a military invasion of Qatar. However, due to the diplomatic efforts of then U.S. secretary of state Rex Tillerson, Saudi Arabia’s plan was thwarted (Emmons, 2018). Leaked e-mails released to the BBC from U.S. businessman Elliott Broidy, a close aide to Donald Trump and the UAE leaders, show that Broidy lobbied the Trump administration in October 2017 to fire Tillerson for his supportive stance toward Qatar. Broidy called Qatar “a television station with a country” in reference to the Al Jazeera channel (Kianpour, 2018, para 15). Trump fired Tillerson later in March 2018 (Emmons, 2018).

The diplomatic rift between Qatar and other GGC states has been manifested on social media; many pro-Qatari Twitter users and trolls changed their profile pictures to show the image of the emir of Qatar with the statement “We’re all Hamad,” while anti-Qatari users employed various hashtags to condemn Qatar, such as “#Qatar supports terrorism” (قطر_تدعم_الأرهاب) or calling the emir’s father “the Gulf’s Qadaffi.” The Saudi information minister claimed that Qatar had hired 23,000 Twitter users to sow division in the region (“The Saudi Information Minister,” 2017). Though it is difficult to prove this claim, political trolls, whether hired or not, have been identified in many regions, including the Middle East. They are often called “online seminars” (Darwish, Alexandrov, Nakov, & Mejova, 2017), “political trolls” (Bradshaw & Howard, 2017), “troll armies,” “electronic armies,” “electronic flies,” or “electronic ghosts” whose main purpose is to intensify the cyberconflict by spamming and disseminating pro-state propaganda.[1] In sum, the many motives behind the diplomatic tension between Qatar and some GCC countries can be attributed to Qatar’s unilateral policies and reluctance to follow Saudi Arabia’s regional strategies. To better understand the GCC cyberconflict, this article examines the cyberoperations and state surveillance in the region.[2]

Literature Review

The concept of and word *hacker* stem from two terms: a *h*obbyist who is curious about how things work and a safecr*acker* who goes beyond curiosity to become someone “who discovers or breaks the established (or secret) code to get into the contents of a safe” (Hirst, Harrison, & Mazepa, 2014, p. 192).[3]

[1] Ghosting (التشبيح) is borrowed from the word *ghost*, which is a reference to the infamous Bashar Assad’s Alawite militia responsible for the kidnapping, blackmail, torture, and killing of many Syrian civilians and members of the opposition. The word stems from the nickname given to the Mercedes cars often driven by members of this militia.

[2] The political tension among GCC countries has extended to cultural productions. Television songs, for example, were swiftly written and produced to criticize Qatar by the Saudi-run channel Rotana as part of this cultural war (Freer, 2017).

[3] *Hacktivism* and *hacking* are often used interchangeably, yet there are clear differences between the two terms. Hacktivism is believed to have “roots in the cyber-libertarian aspects of the Internet,” which originally “began as a movement for the freedom of information” (Siapera, 2012, p. 89; see also Sauter, 2014).

The word *hack* was originally used by MIT students in the 1950s to refer to "a clever, benign, and ethical prank or practical joke, which is both challenging for the perpetrators and amusing to the MIT community" (McQuade, 2009, p. 87). In 1983, *Time* magazine offered a definition of hackers to mean "computer fanatics" (Hirst et al., 2014, p. 191); early hackers were known as "phone phreaks" in the 1970s because they attempted to make free telephone calls (Coleman, 2012). It is important to mention here that the motive behind hacking is one of the defining features of how hackers are categorized. For example, some hackers have financial motives. If they are involved in such illicit activities, they are regarded as cybercriminals provided that they do not have any political goals. For most government agencies, however, hackers are regarded as mere criminals (Hirst et al., 2014, p. 191).

Political hacking is associated with information or cyberwar (Arquilla, 1996; Arquilla & Ronfeldt, 1993; Denning, 1999), which uses different types of technologies to attack opponents' websites. This activity may include unauthorized intrusion into computer systems, distributed denial-of-service attacks, and domain-name-system attacks by utilizing similar cybertools that are used by hacktivists but for different purposes (Siapera, 2012, p. 112). In general, cyberwars can be defined as "aggressive" cyberactivities that attack state, military, or civilian targets (Ventre, 2011, p. ix) or online attacks by one state against another (Jordan, 2008, p. 78). Some scholars distinguish between cyberconflict and cyberwar, where the former means using technologies to achieve militant goals that can influence or possibly change military and diplomatic relations among countries, and the latter is understood to be more serious because it entails the exacerbation of the conflict to reach lethal outcomes such as death and destruction (Valeriano & Maness, 2015, p. 3). Philip Taylor (2002) emphasizes that the virtual or cyber "battle space" has blurred the line between the battle and home fronts because "instantaneous communication technologies are . . . obliterating previous distinctions between tactical and strategic information, and between military and civilian perceptions of what is happening there" (p. 147). Whether cyberwars or cyberconflicts, these operations attempt to gain some advantage (Springer, 2017, p. 70), such as stealing large data troves or destroying an opponent's digital infrastructure. Valeriano and Maness (2015) examined global hacking attempts over 11 years (2001–2011) and found 111 cyberincidents involving rival states. Many rival states engaged in online conflicts are neighbors, suggesting that "cyber conflicts are not disconnected from the typical international conflicts over space and place" (pp. 8–9).

Hacking as Online Political Jamming

This article discusses hacking as a form of online political jamming whose influence flows in a vertical (top-down or bottom-up) or horizontal direction. *Political jamming* is a term derived from culture jamming or cultural jamming, which was introduced in the public sphere by "the 'audio-Dadaism' band Negativeland on a cassette recording called JamCon84 released in 1985 and reissued on CD in 1994" (Cammaerts, 2007a, p. 71). Cultural jamming involves cultural appropriation in a way that subverts the original hegemonic meaning to create confusion, interference, and disruption. Mark Dery (1993) describes culture jamming as a form of "poetic terrorism" as the jammers "introduce noise into the signal as it passes

Dorothy Denning (2001) describes hacktivism as the "marriage of hacking and activism," and the latter is related to the "nondisruptive use of the Internet as a medium that supports a group's cause or agenda" (p. 241). In other words, there is often an ethical dimension in hacktivism (Levy, 1984).

from transmitter to receiver, encouraging idiosyncratic, unintended interpretations. Intruding on the intruders, they invest ads, newscasts, and other media artifacts with subversive meanings" (p. 57). Culture jamming has been applied to resistance against exploitative capitalist practices with the use of mass media (Handelman, 1999), while political jamming is more focused on the cultural politics of such resistance (Jameson, 1992, p. 409) to influence the political process, create awareness, or change policies (Cammaerts, 2007b). Political jamming is "a form of culture jamming that targets not only big corporations but the political in the bad sense" (Bob, Haynes, Pickard, Keenan, & Couldry, 2008, p. 214). Rooted in the language of radio and TV jamming, it is intended to deal with "the messiness of reality, subverting meanings by combining mockery, satire and parody" (Cammaerts, 2007b, p. 214).

Alternative and radical media outlets as well as social movements are often linked to the practice of cultural and political jamming in order to resist mainstream hegemonic ideologies, media, and power (Bailey, Cammaerts, & Carpentier, 2008; Balnaves, Donald, & Shoesmith, 2008, pp. 167, 298; Fontenelle & Pozzebon, 2017). For example, Laura Iannelli (2016), in *Hybrid Politics: Media and Participation*, discusses how political jamming has been used by social activists to "influence media and political agendas, and to engage online and offline publics" (p. 99). Tiffany Derville (2005) notes that radical activist organizations often use "militant communication tactics such as vitriolic rhetoric, disruptive image events, actions that provoke violent backlashes . . . harassment, and sabotage" (p. 529) to resist hegemony and draw attention to their causes.

Accordingly, hacking is another form of militant public communication that serves different goals depending on the nature of the hack. Some scholars confirm the connection between alternative media practices, political jamming, and hacking, citing the example of billboard activists who culturally appropriate billboards to send antihegemonic political messages or Internet users who alter images of George W. Bush to protest against U.S.-led wars (Bailey et al., 2008). Yet Cammaerts (2007a) confirms that the practice of political jamming does not always provide counterhegemonic narratives, because "some political actors . . . just use jamming as a 'hip' political communication strategy, thereby reducing it to a marketing technique" (p. 88). In other words, political jamming is a communication strategy followed by subaltern groups and also by the powerful, "the dominant" (Payne, 2012, p. 65), and the hip. An example of the use of political messages by those who have power is Twitter's release in 2018 of data troves on the social media activities of Russian and Iranian trolls before and after the 2016 U.S. election ("Elections Integrity," 2018). Figure 1 illustrates a form of online political jamming expressing anti-Trump and anti-Saudi attitudes.

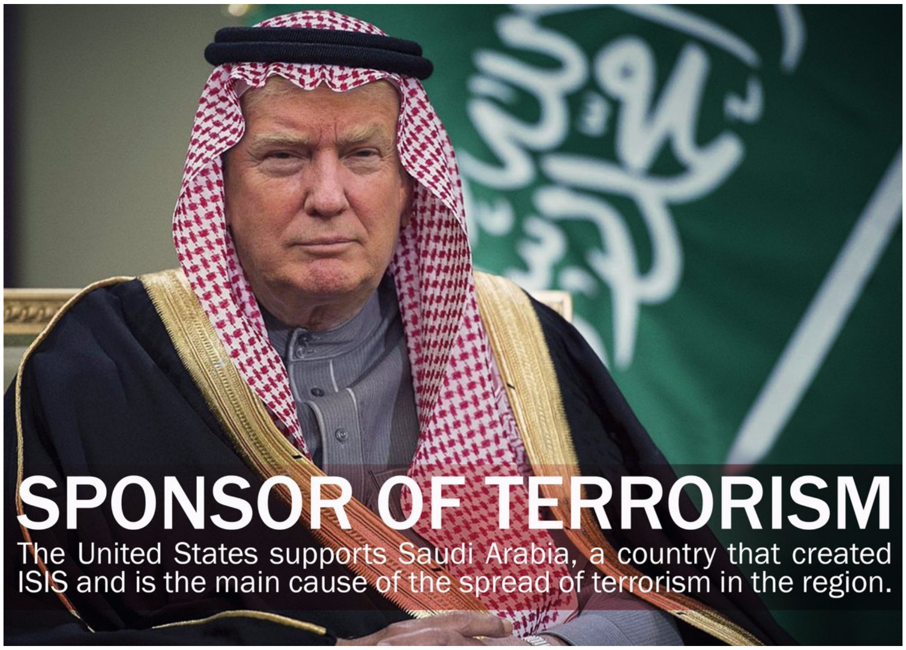
SPONSOR OF TERRORISM
The United States supports Saudi Arabia, a country that created ISIS and is the main cause of the spread of terrorism in the region.

Figure 1. An altered photo of President Donald Trump used by Iranian trolls on Twitter.

I argue here that hacking is a form of political jamming in cyberspace, and I call this activity *online political jamming*. It can be situated as part of Manuel Castells's (2007, 2013) concept of communication power and counterpower in the sense that there are different types of communication flows that shape our networked society. In the model discussed here, I argue that communication powers are represented by nation-states and their cyberwarriors—mercenary hackers as well as other militant cyberoperations—while counterpowers are represented by independent hackers and sometimes global hacktivist groups. Here, the term *cyberwarriors* refers to hackers who "possess the characteristic of being sponsored by states and being subject to the oversight of their governments" (Baldi, Gelbstein, & Kurbalija, 2003, p. 18), such as the many hackers affiliated with the Syrian Electronic Army (Al-Rawi, 2014). In general, nation-states as well as their affiliated hacking groups employ hacking as offensive and defensive tools in connection to the cyberactivity or -inactivity of other nation-states. This is regarded as a horizontal flow of online political jamming. Sometimes nation-states use hacking and surveillance as a vertical flow (top-down) form of online political jamming by targeting their own citizens due to their political views (as explained below). Though it is not related to the focus of this study, regular hacktivists or hip hackers, who are often politically independent, practice a form of bottom-up political jamming when they attempt to hack government websites to address the internal politics of their respective nations, sometimes aided by global hacktivist groups such as Anonymous. Stefania Milan (2015) argues that hacktivism is a form of alternative and radical media practice because of its means and democratic potential. In a horizontal form of online political jamming, the same hackers might target ordinary citizens to express opposition to their political or ideological views. In GCC countries' hacking attempts, there is a clear horizontal form of online political jamming because of the relatively equal power and outreach of these nation-states (see Figure 2).

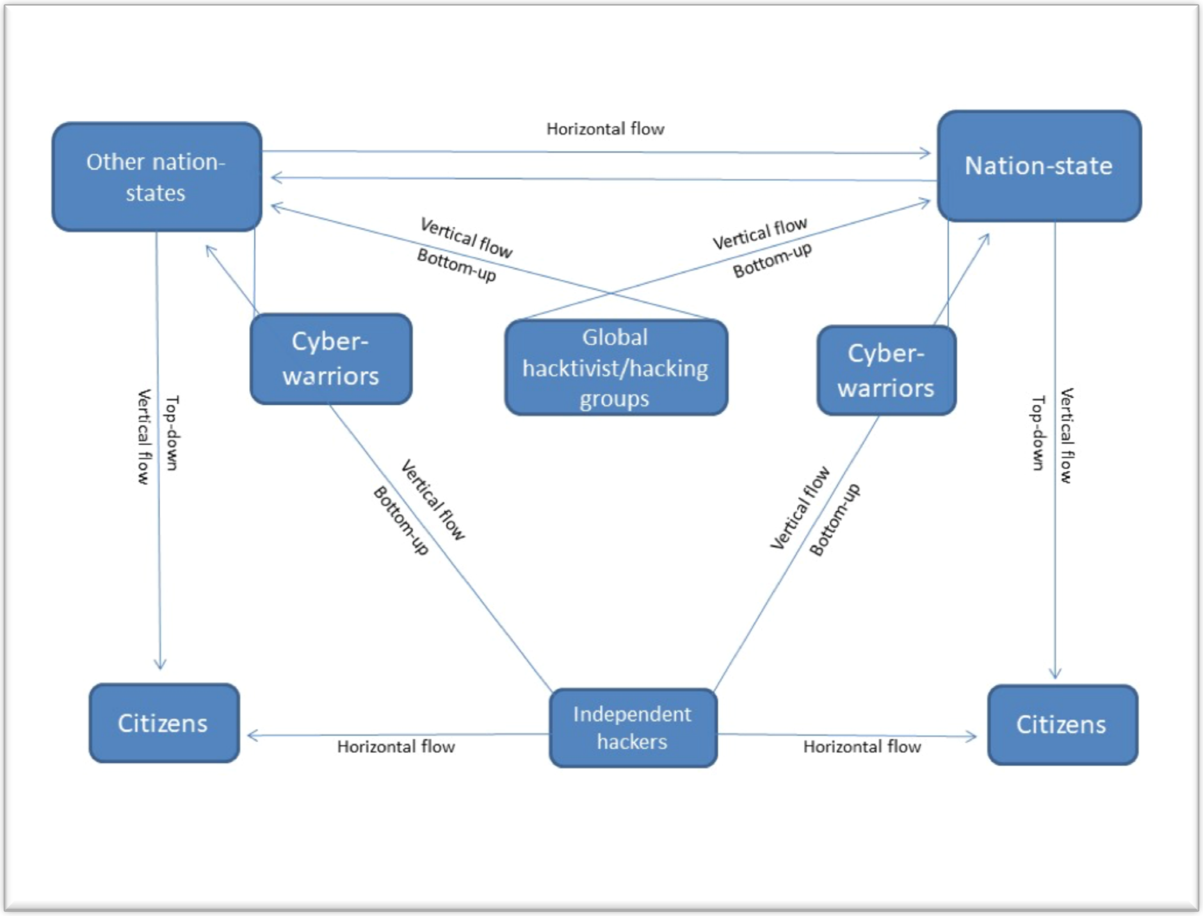

Figure 2. Online political jamming model and hacking.

In sum, hacking is a form of aggressive and militaristic public communication because hackers practice online political jamming and are sometimes sponsored, supported, or employed by states to achieve political goals (Hirst et al., 2014). The definition in this article of the term *cyberconflict* does not follow the traditional definition of armed conflict or military aggression because of the unconventional methods that are employed; yet evidence shows that many neighboring rival states engage in frequent hostile activities due to disagreements or clashes over their geopolitical or economic interests. The next section provides an analytical account of the Qatari hacking incident.

Surveillance States and Cyberconflicts

The cyberconflict discussed here has been facilitated by various technological developments as most governments around the world, including those in the GCC region, have become increasingly reliant on the Internet. This progress has come with a price as many governments routinely face tremendous challenges in protecting their online infrastructures from hackers. It is estimated that billions of dollars are spent on online protection in the Middle East due to the ongoing cyberthreats that many countries face. Jordan, for instance, claims that it countered 70 million cyberattacks in 2016 alone ("Jordan Counters," 2017). In November 2017, the Saudi National Cyber Security Center announced that the kingdom faced a fierce cyberespionage campaign by a hacking group called MuddyWater that affected five other countries in the Middle East ("Saudi Arabia Targeted," 2017). These concerns have prompted governments to enhance their defensive as well as offensive cyberoperations, and many "have adopted laws that purport to combat cybercrimes and terrorism. However, these laws also serve as conduit to curb citizens' rights and freedom" (Khan, 2012, p. 19). This reality has led to many autocratic countries in the region becoming surveillance states (Weller, 2012). The OpenNet Initiative observed in 2009 that the Middle East and North Africa region is one of the "most heavily censored regions in the world" ("Internet Filtering," 2009, p. 2). In the years since then, the region has become more censored due to technological advancement, often with cyberlaws that are ambivalent. For instance, the UAE criminalizes hacking (p. 28), though the government itself is often implicated in hacking activities, and many other Arab countries, such as Saudi Arabia, have laws that penalize hacking but often target political dissent.

A few years before the cyberconflict that is the subject of this article, several GCC countries purchased expensive hacking tools and hired services from foreign companies such as NSO Group and Cellebrite in Israel, FinFisher in Germany, and the Hacking Team in Italy to train security and intelligence officers to hack electronic devices and crack encrypted messages (Perlroth, 2016). Among the Hacking Team's clients were many Arab governments, including those of Morocco, Bahrain, Sudan, Saudi Arabia, and the United Arab Emirates (Hern, 2015). Human Rights Watch (2016) found evidence of "intrusion software" purchased from other sources by Oman and Qatar. The Bahraini government bought "FinSpy, a commercial trojan from the FinFisher suite of surveillance tools sold by Gamma Group International" (Boire, 2012, para. 2) to target Shiite dissidents inside and outside the kingdom (Boire, 2012). Further, the Lebanese intelligence agency known as the General Security Directorate used an Android app to spread malware to spy on activists, military personnel, and journalists for about six years in 20 countries to steal phone records, photos, and other private mobile data ("Data-Stealing Spyware," 2018; Perlroth, 2018). The British firm BAE Systems sold "a mass surveillance software called Evident" ("UK Arms Firm Sold Spyware," 2017, para. 2) that was used to spy on human rights activists, and its clients included Saudi Arabia, the UAE, Qatar, Oman, Morocco, and Algeria. Ironically, these Western-made spying tools were provided to autocratic states mostly to silence pro-democracy activists at a time when many Western governments publicly urge these Arab states to implement democratic reforms.

The UAE and Saudi Arabia are undoubtedly ahead of many other countries in the Arab world in terms of their offensive cybercapabilities (Perlroth, 2016). This lead position is mostly related to these two countries' concern over their national and economic security as well as their desire to quell internal political dissent. One of the first surveillance controversies was related to BlackBerry use in the UAE in 2010 (Gapper, 2010) as the nation pressured Research in Motion, the Canadian maker of the mobile device, to hand over the encryption software in order "to monitor e-mails and messages" (Gapper, 2010, para. 5). The UAE also asked to "maintain servers within the country so that, when it identifies someone who is acting suspiciously, it can find out what else he or she has been up to" (Gapper, 2010, para. 6). Saudi Arabia demanded similar measures to be taken in the kingdom (Gapper, 2010). As part of its current surveillance and cyberoffensive strategies, the UAE hired the services of DarkMatter to monitor all Emirati citizens and foreigners visiting and/or working in the country (McLaughlin, 2016).[4] Another UAE hacking company, the Royal Group, is made up of "a conglomerate run by a member of the Al Nahyan family, one of the six ruling families of the Emirates" (Perlroth, 2016, para. 10), and its spyware was sold by FinFisher and the Hacking Team. Invoices from 2015 show that the UAE paid the Hacking Team alone more than $634,500 to use the spyware on 1,100 targets (Perlroth, 2016).[5]

Indeed, the surveillance and spying technologies used by the UAE and Saudi Arabia have assisted in the hacking attempts against opposition figures. The UAE government sought a spying software update from NSO Group, an Israel-based company that sells Pegasus, a government-exclusive intercept spyware product (Menn, 2016), in order to monitor perceived state opponents. The Emirati government wanted evidence that the software works and requested phone recordings of the Qatari emir, the prime minister of Lebanon Saad Hariri, a Saudi prince, and the editor of an Arabic newspaper based in London. In response, the company offered two phone recordings as evidence, according to leaked e-mails provided by a Qatari journalist to *The New York Times* (Kirkpatrick & Ahmed, 2018). The hacked e-mails show that the UAE government monitored the phone devices of 159 members of the Qatari royal family as well as other officials; later, an assistant to the chairman of the UAE intelligence agency e-mailed his director to confirm that the devices were infected with Pegasus (Kirkpatrick & Ahmed, 2018).

Well-known Emirati human rights advocate Ahmed Mansoor has been repeatedly targeted with cyberattacks to steal information from his electronic devices and ultimately silence him (Groll, 2016). Often called the "million dollar dissident" due to the estimated amount of money spent to hack his electronic devices, Mansoor was targeted with spyware sold by FinFisher and the Hacking Team (Franceschi-Bicchierai, 2016). As a consequence, he was "jailed and fired from his job, along with having his passport confiscated, his car stolen, his email hacked, his location tracked and his bank account robbed of $140,000. He has also been beaten, twice, in the same week" (Perlroth, 2016, para. 1). What happened to Mansoor is an example of vertical (top-down) online political jamming practiced by a state against a dissident citizen to disrupt and create chaos in the person's online, and ultimately off-line, life. As Mansoor's political activism was severely restricted, other human rights activists were targeted by e-mails sent from a fake organization called the

[4] Faisal Al Bennai, the chief executive officer of DarkMatter, used to work as the country's vice president of National Electronic Security Authority (NESA), which is responsible for providing sensitive intelligence to the state. Currently, DarkMatter and NESA work closely together in cyberespionage as the former has employed "an army of cyberwarriors from abroad to conduct mass surveillance aimed at the country's own citizens" (McLaughlin, 2016, para. 10). The company is allegedly interested in "exploiting hardware probes installed across major cities for surveillance, hunting down never-before-seen vulnerabilities in software, and building stealth malware implants to track, locate, and hack basically any person at any time in the UAE" (McLaughlin, 2016, para. 12).

[5] The UAE government allegedly provided the Egyptian leader Abdulfatah El-sisi with a French-made spying tool to monitor Egyptian citizens. The UAE is interested in supporting the current Egyptian government because both countries oppose the Muslim Brotherhood who are regarded as a security threat. The espionage tool was estimated to be worth about €10 million ("The UAE Gives El-Sisi," 2017).

Right to Fight, asking them to click on suspicious links related to human rights issues in the UAE (Perlroth, 2016).

In Saudi Arabia, the assassination of Saudi journalist Jamal Khashoggi in October 2018 revealed more details about the surveillance and hacking activities of the Saudi government against him and many other human rights activists. As mentioned earlier, the Saudi government had hired the services of several Western hacking companies that trained Saudi intelligence agents to spy on Saudi citizens. One of the prominent figures who led the Saudi kingdom to purchase spying tools and hire trolls and hackers is Saud al-Qahtani, a media adviser to the Saudi crown prince who previously worked at the Center for Media Monitoring and Analysis at the Saudi Royal Court (Franceschi-Bicchierai, 2018). Earlier, al-Qahtani had shown interest in hacking culture as an active member of the Hack Forums online community (Franceschi-Bicchierai, 2018). In 2016 and one year after the e-mail leak of the Hacking Team, the company was about to go bankrupt, but al-Qahtani convinced the Saudis to purchase 20% of the company's shares to save it (Franceschi-Bicchierai, 2018). Though al-Qahtani was recently fired, he is still known as Saudi Arabia's Steve Bannon ("Who Is Saud al-Qahtani," 2017), Mr. Hashtag (Franceschi-Bicchierai, 2018), or Prince of Darkness (Kerr, Raval, & England, 2018) due to his efforts to create an army of bots and trolls or electronic flies to combat state dissidents and supporters of Qatar (Kerr, Raval, & England, 2018). These cyberoperations were not confined to the Saudi Kingdom; *The Citizen Lab* reported that Omar Abdulaziz, a Saudi human rights activist residing in Montreal and one of Khashoggi's friends, was successfully targeted by the Saudi government with Pegasus spyware (Marczak, Scott-Railton, Senft, Abdul Razzak, & Deibert, 2018). Again, this is typical of vertical (top-down) online political jamming used by the Saudi government against human rights activists to disrupt their lives and silence them. Further, al-Qahtani was also responsible for creating the viral Arabic hashtag #TheBlacklist on August 17, 2017 ("Who is Saud al-Qahtani, the fired Saudi," 2018), a few months after the Qatari crisis, asking Saudis to add the names of any Qatari sympathizer or "traitors" to the infamous Twitter list (Al Ali, 2018). Finally, it is believed that al-Qahtani masterminded the killing of Khashoggi at the Saudi consulate in Istanbul and gave orders to his aides over Skype ("How the Man Behind Khashoggi," 2018). One of the assassins was a Saudi intelligence officer named Maher Abdulaziz Mutreb, or "dark face," who was trained to use spying technologies in Riyadh and presumably in Italy by the Hacking Team ("Jamal Khashoggi," 2018).

When WikiLleaks released a series of Spy Files containing a trove of hacked documents and e-mails from FinFisher (formerly known as Gamma Group International) and the Hacking Team (https://wikileaks.org/spyfiles/) on September 15, 2014, more important details emerged. An examination of these files reveals that almost all Arab states have purchased services from these two hacking companies. For instance, the Bahraini National Security Agency and Defense Forces were interested in the Hacking Team services ("Re: R: New Opportunity," 2014). Requests from and references to other security bodies that needed the Remote Control System (RCS) Galileo, a tool which provides a backdoor to monitor the computer desktop, phone, and work computer, included the Royal Omani Police, the Emirati Armed Forces, and the Kuwaiti Ministry of Interior. In Saudi Arabia, contacts were made between the Hacking Team and the Ministries of Defense and Aviation, the Center for Media Monitoring and Analysis at the Saudi Royal Court in the King's Office, and the Ministry of Interior–Saudi Interpol. An officer from the Qatari State Security Bureau was periodically in contact with FinFisher to request training on hacking, and the Qatari state was charged a total of €1,945,140 for 890 targets ("Re: Hackers Training," 2015). In brief, the UAE and Saudi

Arabia are not alone in using sophisticated spying tools to monitor foreigners and citizens. Hacking electronic devices to gain valuable political information is largely at the disposal of autocratic states to be used against their opponents. To situate the discussion of the Qatari hacking crisis, the next section provides an account of the concepts of hacking and cyberwar and conflict.

Cyberoperations and the Qatari Hacking Crisis

As mentioned earlier, Valeriano and Maness (2015) show that many cyberconflicts occur among rival neighboring states—a notion that corresponds with the case study reported in this article. The conflict between Qatar and some GCC countries did not escalate into a full-fledged cyberwar because the intention behind the hacking of the Qatari News Agency (QNA) website (which is discussed below) seems to be focused on influencing or changing diplomatic relations between countries (Valeriano & Maness, 2015), which is an obvious example of a cyberconflict. In other words, the hacking of the QNA website is a form of horizontal political jamming intended to disrupt the diplomatic relations among GCC states.

The geopolitical context described in this article's introduction ultimately paved the way for hacking QNA's website and its social media outlets shortly after Donald Trump's visit to Saudi Arabia. According to multiple reports, the hacking, which occurred at 12:13 a.m. on May 24, 2017, had been engineered and orchestrated by the UAE and Saudi Arabia and used as a pretext to cut diplomatic ties with Qatar (Kareem & Ryan, 2017). Senior Emirati officials allegedly discussed the details of the hacking plan and its execution on May 23 (DeYoung & Nakashima, 2017), and the Qatari Interior Ministry claimed that the hacking was traced to two IP addresses located in the UAE that exploited a security vulnerability and installed a malicious program in the QNA site.[6] Doha later claimed that it identified 122 people implicated in the hacking incident, including hackers living in Turkey and some Arab countries such as Egypt and Saudi Arabia ("Turkey Arrests Five Persons," 2017). The fake news story posted by the hackers references the emir of Qatar, Sheikh Tamim Bin Hamad al-Thani, and alleges that he praised Hamas and Iran and suggested that Trump might not last long in office (DeYoung & Nakashima, 2017; "United Arab Emirates," 2017). The surprising issue is that, within 20 minutes, Saudi and Emirati TV channels started airing the details of the fake news story as real and began "interviewing long lines of well-prepared commentators to expound on the perfidy of Qatar" (Kirkpatrick & Frenkel, 2017, para. 2). Due to the timing and logistical difficulties of obtaining such hardline responses in a region that is known for its official media censorship and sensitive political environment, this provides further evidence that the hacking operation was carefully planned by the UAE and Saudi Arabia.

Other decisive diplomatic measures were followed to further isolate Qatar. Saudi Arabia blocked access to the Qatari websites of Al Jazeera, Asharq, Al-Raya, and Al-Arab the next day ("Lifting the Ban," 2017), and the UAE, Bahrain, and Egypt followed the Saudis' lead (DeYoung & Nakashima, 2017). Hacking incidents and spreading fake news have not stopped, which could be regarded as an escalation of regional cyberconflict and online political jamming. During the crisis, the website and social media outlets of Al

[6] The hackers managed to take control of the news agency's social media outlets and posted a fake news story and a YouTube video. At 3:00 a.m., Qatari authorities regained control of the website, and at 7:00 p.m., they managed to restore the social media outlets. The Qatari Interior Ministry claimed that an iPhone device with a European phone number was used in the hacking ("An iPhone," 2017).

Jazeera TV were subjected to multiple hacking attempts (McKernan, 2017), and another fake news story claiming that "six Arab nations had demanded Fifa strip Qatar of the 2022 World Cup" (Harwood, 2017, para. 21) appeared on May 28. Online spammers succeeded in virally disseminating this story, even leading Reuters and a Swiss news agency to publish it (Harwood, 2017). The ongoing cyberconflict did not end at this stage, and other hacking attempts were made. Hacked mobile audio and text messages from Zayed bin Saeed al-Khayareen, Qatar's ambassador to Iraq, were published on April 28, 2018, by *The Washington Post*. The messages detailed the ransom paid by Qatar to free its nationals in Iraq. Though the identities of the hackers were not disclosed, the following statement appeared in the report: "The intercepted communications also include cellphone conversations and voice-mail messages in Arabic that were played for Post reporters for authentication purposes, on the condition that the name of the foreign government that provided the materials not be revealed" (Warrick, 2018, para. 12). The foreign government involved in this hacking incident is most likely Saudi Arabia or the UAE due to their interest in disseminating such information. Because these cyberoperations involved the use of bots and spamming and spreading fake news and were orchestrated and conducted by states and/or their affiliates against Qatar, they present a horizontal form of online political jamming to undermine a country's credibility and influence its foreign policy.

On the other hand, there have been a number of counter-cybermeasures. Qatar seems to have sought the option of hiring mercenary hackers who freelance "for all sorts of different clients, and adapting their skills as needed" (Kirkpatrick & Frenkel, 2017, para. 12). For example, Al Otaiba's e-mail was hacked on June 2, 2017; the hackers used phishing techniques to allure their victims into clicking on certain links. Other Emirati diplomats and public figures in the Gulf region received similar messages in the same time period (Kirkpatrick & Frenkel, 2017). Al Otaiba's leaked e-mails—which were handed over to *The Intercept*, *The Daily Beast*, *Al Jazeera*, and *HuffPost* (Jilani & Emmons, 2017)—were released by GlobaLeaks, which is affiliated with the website of DCLeaks. This incident did not appear to be a coincidence, because the hacked e-mails were "distributed by a group apparently sympathetic to Qatar" (Kareem & Ryan, 2017, para. 26) and defended the Qatari state against various accusations. Incidentally, this was not the first time that leaked documents from the UAE publicly emerged. In 2015, internal e-mails hacked from the Emirati Foreign Ministry were provided to *The New York Times* from an Arab intermediary with ties to Qatar (Kirkpatrick & Frenkel, 2017). The e-mails mentioned that "the U.A.E. was knowingly violating a United Nations resolution by shipping weapons to Libyan militias" (Kirkpatrick & Frenkel, 2017, para. 8). Some of these e-mails appeared in *The Guardian* newspaper and on Qatari-sponsored sites and were meant to pressure the UAE to change its policies in Libya, which were not aligned with Qatar's. These hacking incidents were meant to disclose embarrassing information that could reveal the cybervulnerability of the UAE (and Saudi Arabia) and could clear Qatar from any terrorism-related charges.[7] The e-mail account of Elliott Broidy, cited above, was also allegedly hacked by Qatari-affiliated hackers (Mazzetti, Kirkpatrick, & Haberman, 2018), because cybersecurity experts found similarities between this incident and the one involving Al Otaiba's hacked e-

[7] Qatar also created a "Lift the Blockade" website in September 2017 to target audiences to send countermessages to those prepared by their Saudi and Emirati counterparts (Freer, 2017). Qatar also filed a lawsuit against SkyNews Arabia and Al Arabiya in London because the news outlets continued to air "fake news" about Qatar even though the country strongly denied any connection on its QNA website ("Qatar Files a Lawsuit," 2017).

mails (Kianpour, 2018). Figure 3 shows how the online political jamming model applies to the Qatari crisis. There is a clear form of horizontal jamming among some nation-states as they attempt to pressure each other's governments and influence policies. On the other hand, there is a vertical (top-down) flow of online political jamming and surveillance practiced by nation-states against their own citizens to monitor, disrupt, and curb dissent and political activism.

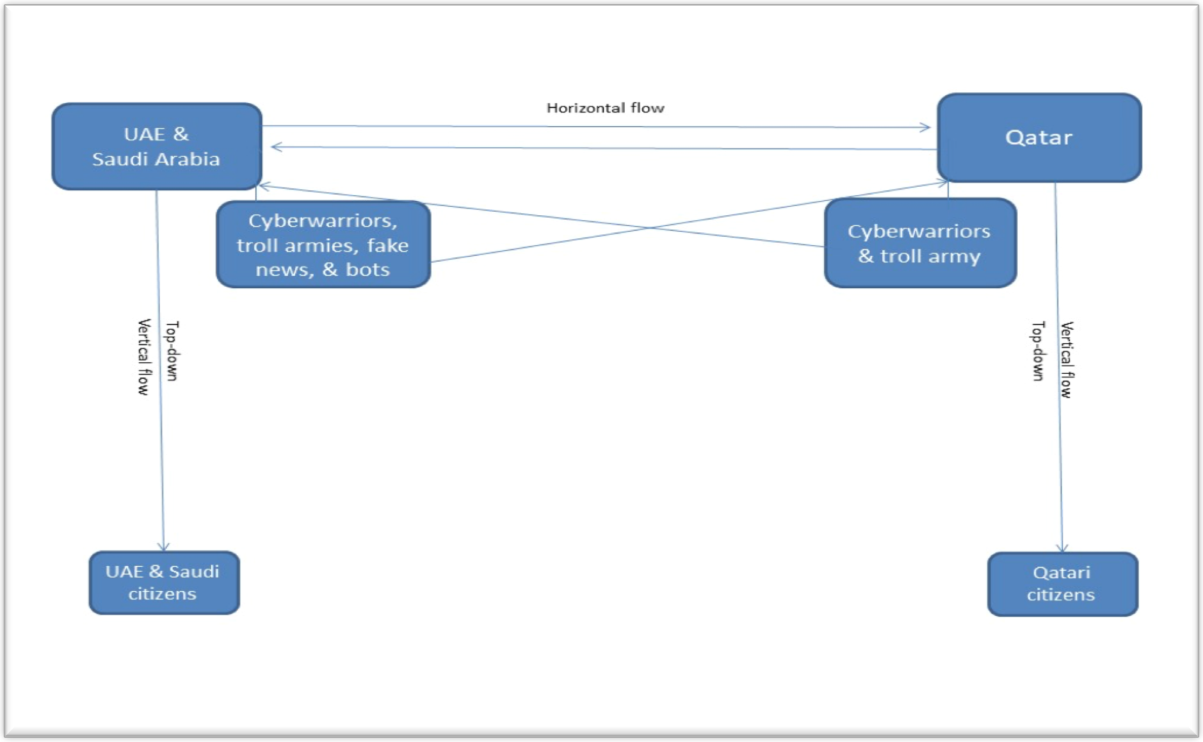

Figure 3. Online political jamming model applied to the GCC context.

Conclusion

The Qatari QNA website was hacked by the UAE in coordination with Saudi Arabia as a way to politically and diplomatically isolate and pressure Qatar and undermine its influence in the region. This hacking incident coincided with the new wave of foreign policies implemented by Saudi Arabia's crown prince, which included intensifying diplomatic tensions against Iran (Zilber, 2017). Indeed, the majority of Arab countries—especially the wealthy ones in the Gulf region—have purchased, used, or employed cyberoffensive measures, surveillance tools, and spying techniques to hack their rivals as well as monitor and target dissidents and human rights activists. These hacking and surveillance acts are examples of vertical (top-down) online political jamming activities, which are meant to compromise, undermine, weaken, and pressure oppositional groups and members. Several Arab countries created offensive cyberdivisions to gather intelligence and hack their enemies—mostly their neighbors—as part of their horizontal political jamming operations. The UAE and Saudi Arabia, in particular, seem to be more advanced than the others in the area of offensive cyberoperations, but neighboring states (such as Qatar) that maintain an opposite stance on some political issues have actively used hacking methods to undermine one another. This is an ongoing cyberconflict that closely corresponds with geopolitical developments in the region, and it "has the potential to escalate" (Valeriano & Maness, 2015, p. 96). The situation is likely to increase in magnitude and multitude due to rapid developments in spying tools and increasing demands for hacked data by autocratic states that continuously seek to quell internal and external dissent.

References

Al Ali, N. (2018, October 24). Fired Saudi royal court adviser drops all titles in Twitter bio. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2018-10-24/fired-saudi-royal-court-adviser-drops-all-titles-in-twitter-bio

Al-Rawi, A. (2014). Cyber warriors in the Middle East: The case of the Syrian Electronic Army. *Public Relations Review*, *40*(3), 420–428.

Al-Rawi, A. (2015). Sectarianism and the Arab Spring: Framing the popular protests in Bahrain. *Global Media and Communication*, *11*(1), 25–42.

Al-Rawi, A. (2017). Assessing public sentiments and news preferences on Al Jazeera and Al Arabiya. *International Communication Gazette*, *79*(1), 26–44.

An iPhone with a European number was used in the hacking. (2017, July 20). *HuffPost Arabi*. Retrieved from http://www.huffpostarabi.com/2017/07/20/story_n_17541988.html

Arango, T. (2017, April 21). Big ransom and Syria deals win release of royal Qatari hunters. *The New York Times.* Retrieved from https://www.nytimes.com/2017/04/21/world/middleeast/big-ransom-and-syria-deals-win-release-of-royal-qatari-hunters.html

Arquilla, J. (1996). *The advent of netwar*. New York, NY: Rand Corporation.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, *12*(2), 141–165.

Bailey, O., Cammaerts, B., & Carpentier, N. (2008). *Understanding alternative media*. New York, NY: Open University Press.

Baldi, S., Gelbstein, E., & Kurbalija, J. (2003). *Hacktivism, cyber-terrorism and cyberwar: The activities of the uncivil society in cyberspace.* Msida, Malta: Diplo Foundation.

Balnaves, M., Donald, S., & Shoesmith, B. (2008). *Media theories and approaches: A global perspective*. Hampshire, UK: Palgrave Macmillan.

Bob, C., Haynes, J., Pickard, V., Keenan, T., & Couldry, N. (2008). Media spaces: Innovation and activism. In M. Albrow, A. Helmut, M. Glasius, M. Price, & M. Kaldor (Eds.), *Global civil society 2007/8: Communicative power and democracy* (pp. 198–223). Thousand Oaks, CA: SAGE Publications.

Boire, M. (2012, October). Backdoors are forever: Hacking team and the targeting of dissent. *The Citizen Lab*. Retrieved from https://citizenlab.ca/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/

Bradshaw, S., & Howard, P. (2017). *Troops, trolls and troublemakers: A global inventory of organized social media manipulation* (Working paper no. 2017.12). Oxford, UK: University of Oxford Computational Propaganda Research Project.

Cammaerts, B. (2007a) Jamming the political: Beyond counter-hegemonic practices. *Continuum: Journal of Media and Cultural Studies*, *21*(1), 71–90.

Cammaerts, B. (2007b). Political jamming. In H. Anheier, M. Glasius, & M. Kaldor (Eds.), *Global civil society 2007/8: Communicative power and democracy* (pp. 214–215). London, UK: SAGE Publications.

Castells, M. (2007). Communication, power and counter-power in the network society. *International Journal of Communication*, *1*(1), 29.

Castells, M. (2013). *Communication power*. Oxford, UK: Oxford University Press.

Coleman, G. (2012). Phreaks, hackers, and trolls: The politics of transgression and spectacle. In M. Mandiberg (Ed.), *The social media reader* (pp. 99–119). New York, NY: New York University Press.

Darwish, K., Alexandrov, D., Nakov, P., & Mejova, Y. (2017, September). Seminar users in the Arabic Twitter sphere. *International Conference on Social Informatics* (pp. 91–108). Oxford Internet Institute. Oxford, UK: Springer.

Data-stealing spyware “traced to Lebanon.” (2018, January 19). *BBC News*. Retrieved from https://www.bbc.com/news/technology-42746772

Denning, D. (1999). *Information warfare and security* (Vol. 4). Reading, MA: Addison-Wesley.

Denning, D. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 239–288). Santa Monica, CA: Rand Corporation.

Derville, T. (2005). Radical activist tactics: Overturning public relations conceptualizations. *Public Relations Review*, *31*(4), 527–533.

Dery, M. (1993). *Culture jamming: Hacking, slashing, and sniping in the empire of signs* (Vol. 25). Westfield, NJ: Open Media.

DeYoung, K., & Nakashima, E. (2017, July 16). UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to U.S. intelligence officials. *The Washington Post*. Retrieved from 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?utm_term=.a8fae1e2fb93

Elections integrity: Twitter's focus is on a healthy public conversation. (2018). *Twitter*. Retrieved from https://about.twitter.com/en_us/values/elections-integrity.html#data

Emmons, A. (2018, August 1). Saudi Arabia planned to invade Qatar last summer: Rex Tillerson's efforts to stop it may have cost him his job. *The Intercept.* Retrieved from https://theintercept.com/2018/08/01/rex-tillerson-qatar-saudi-uae/

Fontenelle, I., & Pozzebon, M. (2017). Jamming the jamming: Brazilian protests as an illustration of a new politics of consumption. *Culture and Organization*, 1–15. doi:10.1080/14759551.2017.1397670

Franceschi-Bicchierai, L. (2016, August 26). The "million dollar dissident" is a magnet for government spyware. *Motherboard.* Retrieved from https://motherboard.vice.com/en_us/article/mg7pjy/ahmed-mansoor-million-dollar-dissident-government-spyware

Franceschi-Bicchierai, L. (2018, October 29). How "Mr. Hashtag" helped Saudi Arabia spy on dissidents. *Motherboard.* Retrieved from https://motherboard.vice.com/en_us/article/kzjmze/saud-al-qahtani-saudi-arabia-hacking-team

Freer, C. (2017, October 10). Social effects of the Qatar crisis. *Indrastra Global.* Retrieved from http://www.indrastra.com/2017/10/Social-Effects-of-Qatar-Crisis-003-10-2017-0013.html

Gapper, J. (2010, August 4). Keep the spies from our computers. *Financial Times.* Retrieved from https://www.ft.com/content/bfe23646-9ff6-11df-8cc5-00144feabdc0

Grim, R. (2017, August, 10). Gulf government gave secret $20 million gift to D.C. think tank*. The Intercept.* Retrieved from https://theintercept.com/2017/08/09/gulf-government-gave-secret-20-million-gift-to-d-c-think-tank/

Grim, R., & Walsh, B. (2017, November 9). Leaked documents expose stunning plan to wage financial war on Qatar—and steal the World Cup. *The Intercept.* Retrieved from https://theintercept.com/2017/11/09/uae-qatar-oitaba-rowland-banque-havilland-world-cup/

Groll, E. (2016, August 25). The UAE spends big on Israeli spyware to listen in on a dissident. *Foreign Policy*. Retrieved from https://foreignpolicy.com/2016/08/25/the-uae-spends-big-on-israeli-spyware-to-listen-in-on-a-dissident/

Handelman, J. (1999). Culture jamming: Expanding the application of the critical research project. In E. J. Arnould & L. M. Scott (Eds.), *Advances in consumer research* (Vol. 26, pp. 399–404). Provo, UT: Association for Consumer Research.

Harwood, A. (2017, July 18). The Qatari hack cements the Middle East as the worst region in the world for fake news. *The Independent*. Retrieved from http://www.independent.co.uk/voices/qatar-uae-saudi-arabia-fake-news-middle-easy-worst-in-world-a7846571.html

Hedges, M., & Cafiero, G. (2017). The GCC and the Muslim Brotherhood: What does the future hold? *Middle East Policy*, *24*(1), 129–153.

Hern, A. (2015, July 6). Hacking team hacked: Firm sold spying tools to repressive regimes, documents claim. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim

Hirst, M., Harrison, J., & Mazepa, P. (2014). *Communication and new media: From broadcast to narrowcast*. Don Mills, Canada: Oxford University Press Canada.

How the man behind Khashoggi murder ran the killing via Skype. (2018, October 22). *Reuters.* Retrieved from https://www.reuters.com/article/us-saudi-khashoggi-adviser-insight/how-the-man-behind-khashoggi-murder-ran-the-killing-via-skype-idUSKCN1MW2HA

Human Rights Watch. (2016). *140 characters*. Retrieved from https://features.hrw.org/features/HRW_2016_reports/140_Characters/index.html

Iannelli, L. (2016). *Hybrid politics: Media and participation*. Thousand Oaks, CA: SAGE Publications.

Internet filtering in the Middle East and North Africa. (2009). *OpenNet Initiative*. Retrieved from http://opennet.net/sites/opennet.net/files/ONI_MENA_2009.pdf

Jamal Khashoggi: Saudi murder suspect had spy training. (2018, October 19). *BBC News*. Retrieved from https://www.bbc.com/news/world-middle-east-45918610

Jameson, F. (1992). *Postmodernism, or the culture of late capital*. Durham, NC: Duke University Press.

Jilani, Z., & Emmons, A. (2017, July 30). Hacked emails show UAE building close relationship with D.C. think tanks that push its agenda. *The Intercept*. Retrieved from https://theintercept.com/2017/07/30/uae-yousef-otaiba-cnas-american-progress-michele-flournoy-drone/

Jordan counters 70 million cyber attacks in one year. (2017, November 11) *HuffPost Arabi*. Retrieved from http://www.huffpostarabi.com/2017/11/20/story_n_18601654.html

Jordan, T. (2008). *Hacking: Digital media and technological determinism*. Oxford, UK: Polity Press.

Kareem, F., & Ryan, M. (2017, August 3). The UAE's hunt for its enemies is challenging its alliance with the United States. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/middle_east/uaes-drive-for-regional-influence-tests-its-military-alliance-with-the-united-states/2017/08/03/448683ee-6bd2-11e7-abbc-a53480672286_story.html?utm_term=.11a1883caaaa

Kerr, S., Raval, A., & England, A. (2018, November 18). Saudi "prince of darkness" lingers in the shadows. *Financial Times*. Retrieved from https://www.ft.com/content/e9940fc8-e9a3-11e8-a34c-663b3f553b35

Khan, S. O. (2012, December 15). 2012 cyberwatch year in review: Middle East and North Africa, Southeast Asia, Latin America and the Caribbean. *The Citizen Lab*. Retrieved from https://citizenlab.ca/2012/12/2012-year-in-review-cyberwatch/

Kianpour, S. (2018, March 5). Emails show UAE-linked effort against Tillerson. *BBC News*. Retrieved from https://www.bbc.com/news/world-us-canada-43281519

Kirkpatrick, D. (2017, July 1). Journalist joins his jailer's side in a bizarre Persian Gulf feud. *The New York Times*. Retrieved from https://www.nytimes.com/2017/07/01/world/middleeast/qatar-egypt-united-arab-emirates-mohamed-fahmy.html

Kirkpatrick, D., & Ahmed, A. (2018, August 31). Hacking a prince, an emir and a journalist to impress a client. *The New York Times*. Retrieved from https://www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html

Kirkpatrick, D., & Frenkel, S. (2017, June 8). Hacking in Qatar highlights a shift toward espionage for hire. *The New York Times*. Retrieved from https://nyti.ms/2s1Ux1x

Lenderking, T., Cammack, P., Shihabi, A., & Des Roches, D. (2017). The GCC rift: Regional and global implications. *Middle East Policy*, *24*(4), 5–28.

Levy, S. (1984). *Hackers: Heroes of the computer revolution*. Garden City, NY: Anchor Press/Doubleday.

Lifting the ban on Qatar websites in Saudi Arabia. (2017, July 24). *HuffPost Arabi*. Retrieved from http://www.huffpostarabi.com/2017/07/24/story_n_17568516.html

Marczak, B., Scott-Railton, J., Senft, A., Abdul Razzak, B., & Deibert, R. (2018, October 1). The kingdom came to Canada: How Saudi-linked digital espionage reached Canadian soil. *The Citizen Lab*. Retrieved from https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/

Mazzetti, M., Kirkpatrick, D., & Haberman, M. (2018, March 3). Mueller's focus on adviser to Emirates suggests broader investigation. *The New York Times*. Retrieved from https://nyti.ms/2F86rdF

McKernan, B. (2017, June 8). Al Jazeera hack: Publisher under cyber attack on all websites, Facebook and Twitter pages. *The Independent*. Retrieved from http://www.independent.co.uk/News/world/al-jazeera-attack-hack-qatar-cyber-facebook-twitter-website-news-a7779826.html

McLaughlin, J. (2016, October 24). Spies for hire: How the UAE is recruiting hackers to create the perfect surveillance state. *The Intercept*. Retrieved from https://theintercept.com/2016/10/24/darkmatter-united-arab-emirates-spies-for-hire/

McQuade, S. (2009). *Encyclopedia of cybercrime*. New York, NY: Greenwood.

Menn, J. (2016, August 25). Apple fixes security flaw after UAE dissident's iPhone targeted. *Reuters*. Retrieved from https://www.reuters.com/article/us-apple-iphone-cyber/apple-fixes-security-flaw-after-uae-dissidents-iphone-targeted-idUSKCN1102B1

Milan, S. (2015). Hacktivism as a radical media practice. In C. Atton (Ed.), *The Routledge companion to alternative and community media* (pp. 550–560). London, UK: Routledge.

Payne, J. (2012). Feminist media as alternative media? Theorising feminist media from the perspective of alternative media studies. In E. Zobl & R. Drüeke (Eds.), *Feminist media: Participatory spaces, networks and cultural citizenship* (pp. 55–72). Berlin, Germany: Transcript-Verlag.

Perlroth, N. (2016, May 29). Governments turn to commercial spyware to intimidate dissidents. *The New York Times*. Retrieved from https://www.nytimes.com/2016/05/30/technology/governments-turn-to-commercial-spyware-to-intimidate-dissidents.html

Perlroth, N. (2018, January 18). Lebanese intelligence turned targets' Android phones into spy devices, researchers say. *The New York Times*. Retrieved from https://nyti.ms/2FRlAB7

Powers, S., & Jablonski, M. (2015). *The real cyber war: The political economy of Internet freedom*. Champaign, IL: University of Illinois Press.

Qatar files a lawsuit against SkyNews Arabia and Al Arabiya in London. (2017, June 19). *HuffPost Arabi*. Retrieved from http://www.huffpostarabi.com/2017/06/19/story_n_17210874.html

Re: hackers training. (2015). *WikiLeaks*. July 8. Retrieved from https://wikileaks.org/hackingteam/emails/emailid/12534

Re: R: New opportunity—Bahrain. (2014). *WikiLeaks*. April 14. Retrieved from https://wikileaks.org/hackingteam/emails/emailid/12802

Saudi Arabia targeted in cyber spying campaign. (2017, November 21). *Gulf News*. Retrieved from http://gulfnews.com/news/gulf/saudi-arabia/saudi-arabia-targeted-in-cyber-spying-campaign-1.2127967

Sauter, M. (2014). *The coming swarm: DDOS actions, hacktivism, and civil disobedience on the Internet*. New York, NY: Bloomsbury.

Sciutto, J., & Herb, J. (2017, July 11). Exclusive: The secret documents that help explain the Qatar crisis. *CNN*. Retrieved from http://www.cnn.com/2017/07/10/politics/secret-documents-qatar-crisis-gulf-saudi/index.html

Siapera, E. (2012). *Understanding new media*. Thousand Oaks, CA: SAGE Publications.

Solomon, E. (2017, June, 5). The $1bn hostage deal that enraged Qatar's gulf rivals. *Financial Times*. Retrieved from https://www.ft.com/content/dd033082-49e9-11e7-a3f4-c742b9791d43

Springer, P. (Ed.). (2017). *Encyclopedia of cyber warfare*. New York, NY: ABC-CLIO.

Steve Bannon says Trump's Saudi visit started Qatar crisis. (2017, October 23). *Middle East Eye*. Retrieved from http://www.middleeasteye.net/news/steve-bannon-says-trumps-visit-saudi-sparked-qatar-blockade-1719031821

Swisher, C., & Grim, R. (2018, March 2). Jared Kushner's real-estate firm sought money directly from Qatar government weeks before blockade. *The Intercept*. Retrieved from https://theintercept.com/2018/03/02/jared-kushner-real-estate-qatar-blockade/

Taylor, P. (2002). *Global communications, international affairs and the media since 1945*. London, UK: Routledge.

The accused live in Arab countries including Saudi Arabia and Egypt. (2017, August 28). *HuffPost Arabi*. Retrieved from http://www.huffpostarabi.com/2017/08/28/story_n_17851342.html

The Saudi information minister: Qatar employs 23,000 Twitter users to sow division. *HuffPost Arabi*. (2017, June 6). Retrieved from http://www.huffpostarabi.com/2017/07/06/story_n_17408562.html

The UAE gives El-Sisi a French espionage system. (2017, November 9). *HuffPost Arabi*. Retrieved from http://www.huffpostarabi.com/2017/11/09/story_n_18513146.html

Turkey arrests five persons suspected of being involved in hacking the Qatari news agency. (2017, August 25). *Al Jazeera*. Retrieved from https://goo.gl/4kvV1d

UK arms firm sold spyware to repressive Middle East states. (2017, June 15). *Middle East Eye*. Retrieved from http://www.middleeasteye.net/news/bae-systems-sold-surveillance-software-used-repression-across-middle-east-report-1614150131

Ulrichsen, K. (2017). The GCC crisis: Regional realignment or paralysis? *Turkish Policy Quarterly*, *16*(3), 71–79.

United Arab Emirates reportedly behind hacking of Qatari media that incited crisis. (2017, July 16). *CNBC*. Retrieved from https://www.cnbc.com/2017/07/16/united-arab-emirates-reportedly-behind-hacking-of-qatari-media-that-incited-crisis.html

Valeriano, B., & Maness, R. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. New York, NY: Oxford University Press.

Ventre, D. (2011). *Cyberware and information warfare*. London, UK: John Wiley.

Warrick, J. (2018, April 28). Hacked messages show Qatar appearing to pay hundreds of millions to free hostages. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/hacked-messages-show-qatar-appearing-to-pay-hundreds-of-millions-to-free-hostages/2018/04/27/46759ce2-3f41-11e8-974f-aacd97698cef_story.html?noredirect=on&utm_term=.ab1557bdf7d2

Weller, T. (2012). The information state: An historical perspective on surveillance. In D. Lyon, K. Ball, & K. Haggerty (Eds.), *Routledge handbook of surveillance studies* (pp. 57–63). London, UK: Routledge.

Who is Saud al-Qahtani, Saudi Arabia's Steve Bannon? (2017, August 23). *The New Arab.* Retrieved from https://www.alaraby.co.uk/english/indepth/2017/8/23/who-is-saoud-al-qahtani-saudi-arabias-steve-bannon-

Who is Saud al-Qahtani, the fired Saudi royal court adviser? (2018, October 20) *Al Jazeera*. Retrieved from https://www.aljazeera.com/news/2018/10/saud-al-qahtani-fired-saudi-royal-court-adviser-181020125449478.html

Why did the 3 GCC countries withdraw their ambassadors from Qatar? (2014, March 5). *Al Arabiya*. Retrieved from https://goo.gl/CGkyuU

Zakheim, D. (2017, November 7). Elephants in the room: Jared Kushner, Mohammed bin Salman, and Benjamin Netanyahu are up to something. *Foreign Policy*. Retrieved from http://webcache.googleusercontent.com/search?q=cache:QdCQDNLWZxEJ:foreignpolicy.com/2017/11/07/jared-kushner-mohammed-bin-salman-and-benjamin-netanyahu-are-up-to-something/+&cd=1&hl=en&ct=clnk&gl=ca

Zilber, N. (2017, July 14). Israel’s secret Arab allies. *The New York Times*. Retrieved from https://www.nytimes.com/2017/07/14/opinion/israels-secret-arab-allies.html?mabReward=ACTM2&recp=1%203/3