G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Policy Brief

2017 | No. 35

Cheap Havoc: How Cyber-Geopolitics Will Destabilize the Middle East

By Kristina Kausch

Over the past few years, governments and non-state groups in the Middle East and North Africa have gone to great lengths to build cyber capabilities. The proliferation of cyber weapons in the region and their use as geopolitical tools has the potential to further shake and unsettle regional crises and larger Western interests.

The biggest risk for Western powers is to leave any doubt about their readiness to retaliate or to support their allies against any actors' cyber aggressions. As actors around the world begin to grasp the opportunities offered by conducting geopolitical operations in cyberspace, the window for showing this readiness is small and closing.

Since a hack on a Qatari government website in June 2017 triggered the Gulf Cooperation Council's (GCC) deepest diplomatic crisis since its inception, the Gulf states have been stepping up their efforts to enhance their cyber reach and keep up with the rapid strides of regional cyber powers Iran and Israel. Planting a seed of misinformation in a bed of long-standing tensions, a fake news story exploited regional polarization and anti-Iranian sentiments to rip the region further apart. The Qatar crisis not only escalated long-simmering tensions in a region key to U.S. and EU interests and put in question its regional security arrangements; it also provided a glimpse of how the pursuit of expansive geopolitical ambitions by means of targeted cyber-attacks can generate conflict and trigger political landslides in the glimpse of an eye.

In the Middle East, global geopolitical trends tend to manifest themselves early, and intensely. Digital innovation offers political adversaries increasing opportunity to find vulnerabilities that have the potential to undo the capacities of a nation's economic and military force. Geopolitics is at a critical inflection point where the cyber domain is becoming a principal frontline. Over the past few years, governments and non-state groups in the Middle East and North Africa (MENA) have gone to great lengths to build cyber capabilities. The proliferation of cyber weapons in the region and their use as geopolitical tools has the potential to further shake and unsettle regional crises and larger Western interests.

The Digital Face of Geopolitics

Most transatlantic debate about cybersecurity from a geopolitical angle has focused on Russia and its interference in Western elections. Russian operations in the United States, France, and across Europe have put on full display the potential to wreak political havoc abroad with the help of the cyber toolbox. With the digitalization of industries, geopolitics — the use of statecraft and assets to gain influence in international affairs[1] — becomes increasingly detached from its original geographical framing. Cyberspace — the global network of interconnected information technology including hardware, software, and information[2] — is host to some of states' greatest geopolitical weapons and vulnerabilities alike. As cyber threats and physical threats become indivisible,[3] "cyber-geopolitics" is likely to be at the forefront of future geopolitical competition.

The cyber toolbox used to pursue geopolitical aims includes a wide range of instruments including those for surveillance, espionage, disinformation, or destructive attacks. Cyber-attacks can roughly be grouped into two types: breaches to gather information (digital espionage), and attacks on foreign systems to block or damage adversaries' networks, such as of governmental bodies, symbolic targets, and critical infrastructure.[4] While it is cheap and comparatively easy for hackers to break into a system, the development of an attack with real-world impact is much more complex and requires capacities that not many powers, let alone non-state actors, may possess. The value of cyber-attacks as a tool of direct coercion is limited given the blurred nature of both the identity of the author and the message behind the attack.[5] In many other respects, however, cyber-attacks have significant advantages on the geopolitical battlefield compared to conventional tools of international influence. They have a high disruptive potential at a comparatively low economic cost for the attacker. Political cost in the form of risk of retaliation is low, too, given the challenges in attributing authorship. The uncertain limbo of transnational cyber operations in international law further render them attractive as norms and penalties remain unclear.[6] Combining high disruptive potential and quick deployment at low political and economic cost, cyber-attacks square nicely for actors who pursue an expansive geopolitical strategy with limited resources and/or defensive capabilities.

> ***"Due to the difficulties of attribution and the related dilemmas of retaliation, the cyber domain presents a challenge to traditional mechanisms of deterrence."***

Due to the difficulties of attribution and the related dilemmas of retaliation, the cyber domain presents a challenge to traditional mechanisms of deterrence. A senior American cyber figure told the U.S. Senate in 2015 that as conventional deterrence was "eroding to a worrisome degree, addressing that risk in the cyberspace domain" was key in order "to preserve the effectiveness of our traditional instruments of national power."[7] In the Middle East, the cyber proliferation of actors with an extensive regional agenda presents a particular challenge.

The MENA Cyber Awakening

The "Year Zero"[8] of cyber geopolitics had its roots in the Middle East. In June 2012, U.S. media published leaked information about an alleged U.S.–Israeli cyber-attack on Iranian nuclear facilities with the Stuxnet virus, first discovered in 2010. The sophisticated worm, believed to be the first time an offensive cyber weapon has caused physical damage to an industrial facility, aimed at curtailing Iran's nuclear ambitions by destroying one-fifth of Iranian uranium centrifuges. In 2011 and 2012, Russia-based Kaspersky Lab discovered two other cyber espionage tools (Duqu and Flame) associated with Stuxnet. In

1 Nayef al-Rodhan, *Neo-statecraft and Meta-geopolitics: Reconciliation of Power, Interests, and Justice in the 21st Century*, New Jersey: Transaction Publishers, 2009, pp. 33-49.

2 Adam Segal, *The Hacked World Order*, New York: Public Affairs, 2016, p. 34.

3 Meredith Wilson, "The Geopolitics–Cyber Nexus," Emergent Risk International, August 14, 2017.

4 John Glaser, "Cyber War on Iran Won't Work," Defense One, August 21, 2017.

5 Ibid.

6 Patryk Pawlak, "A Wild Wild Web? Laws, Norms, Crime, and Politics in Cyberspace," European Union Institute for Security Studies, July 12, 2017.

7 Admiral Michael S. Rogers, Commander, United States Cyber Command, "Statement Before U.S. Senate Committee on Armed Services," September 29, 2015.

8 Segal, 2017, p. 2-10.

the aftermath, a senior Iranian Islamic Revolutionary Guard Corps (IRGC) official has been quoted as characterizing cyber warfare as "more dangerous than a physical war."[9]

For over a decade, Iran has used cyber tools to spy on Iranian dissidents and limit Iranian citizens' access to information. Iran's cyber capabilities have their origin in the patriotic hacktivist collectives of the 2000s that systematically compromised networks of foreign organizations and governments deemed hostile to the Islamic Republic. Many former members of these groups continue their activities today for the regime under the umbrella "Iranian Cyber Army." Events of the 2009 Green Revolution led to the systematic build-up of cyber capacities by the regime to curb internal dissent. It also set up a Linux-based national computer operating system in 2012 a national email service the following year, and by approximately 2019, a national Internet, disconnected from the World Wide Web, is expected to be operational.[10] Since the 2010 Stuxnet operation that exposed Iran's vulnerability to foreign interference via cyberspace, Iran began to devote considerable resources to increasing its cyber arsenal. Over the past decade, the Islamic Republic's cyber activities have "evolved from a low-tech means for lashing out at its enemies to a pillar of its national security concept."[11]

The governmental body overseeing most cyber activities is the Supreme Council of Cyberspace that was established by Ayatollah Khamenei in 2012 with the aim of consolidating cyber decision-making in a single body under his command. The Council is composed by members of the different Iranian intelligence and security agencies. Although the way cyber fits into the different institutions of the Iranian political and defense apparatus remains opaque, a 2016 indictment of seven Iranian hackers by the U.S. Justice Department unequivocally stated that the accused "performed work on behalf of the Iranian government, including the Islamic Revolutionary Guard Corps."[12]

Iran's international cyber activity involves not only espionage and defensive mechanisms but increasingly targeted political disruption for geopolitical ends. These capacities were showcased in August 2012 when, possibly in retaliation for an unidentified virus discovered in the network of Iran's Oil Ministry four months earlier, an Iranian hacker group called Shamoon attacked Saudi Aramco, the world's biggest oil company and the base of Saudi wealth. The destructive malware launched by Shamoon deleted data on three-quarters of Aramco's PCs, branding screens with a picture of a burning American flag. Aramco was forced to shut down its network and destroy some 35,000 computers. Later that year, a hacktivist group unleashed the same wiper virus on Qatar's natural gas authority, GasRas.

> *"While Iran has been identified as the author of 19 state-sponsored offensive cyber operations since 2010, it has also been the target of 18 such operations by others."*

In February 2014, Iran also showed that it was willing to use cyberspace to directly target and intimidate vocal opponents abroad. It attacked the network of Las Vegas Sands Corporation, whose CEO, a staunch supporter of Israel, had publicly suggested launching a nuclear bomb onto Tehran.[13] Iran has also conducted denial-of-service activities that render systems temporarily inaccessible.[14] In 2013 and 2014, Iranian hackers targeted U.S. financial institutions. Perhaps most significantly, Iran has demonstrated its capacity and intention to intrude onto the networks and systems of its rivals' critical infrastructure, such as when it breached the control systems of a small, computerized dam in Rye Brook, New York. While the Islamic Republic has been identified as the author of 19 (publicly known) state-sponsored offensive cyber

9 "Iran Sees Cyber Attacks as Greather Threat Than Actual War," Reuters, September 12, 2012.

10 Michael Eisenstadt, "Iran's Lengthening Cyber Shadow," Washington Institute for Near East Policy, July 2016.

11 Ibid.

12 U.S. District Court, Southern District of New York, "United States of America versus Ahmed Fathi," 2016.

13 Levy Maxey, "Cybersecurity in the Gulf: The Middle East's Virtual Frontline," The Cipher Brief, January, 29, 2017.

14 A denial-of-service (DoS) attack is an attack meant to shut down a machine or network and make it inaccessible to its legitimate users and owners. DoS attacks often target web servers of high-profile organizations such as banking, commerce, trade, media, and government institutions. Although DoS attacks do not usually result in the theft or loss of data, recovering access to the affected network often implies high cost, time and effort for the victim. For further details see Paloalto Networks, "Cyberpedia."

operations since 2010, it has also been the target of 18 such operations by others, putting the often-stressed Iranian cyber prowess into perspective.[15]

Ahead of Iran, Israel has the most significant cyber capabilities in the MENA region, on eye level with the world's first-tier cyber powers United States, Russia, and China. The most seasoned cyber actor in the region, since 2010 Israel has been the target 11 publicly known offensive cyber operations and has been the sponsor of five such operations during the same period.[16] Used to defending itself against smaller hacker attacks, in 2014 Israel allegedly fended off a large-scale strike from Iran during the war with Hamas. U.S. cyber security firms also linked denial-of-service activities against Israel to Iranian hackers (possibly state-sponsored) during and after the 2014 Gaza war.[17] The following year, an Israeli cyber security firm discovered a large-scale cyber-attack campaign targeting military suppliers, telecom companies, media outlets, and universities in Israel and a dozen other countries with malware meant to steal sensitive data. The firm suspected the Iranian proxy Hezbollah of being behind the attack, marking a shift in the scope of Israel's digital battle with its regional adversaries.[18]

> ***"Israel has the most significant cyber capabilities in the MENA region."***

In 2012, the Israeli government established a National Cyber Bureau and later, in 2015, the National Cyber Authority as a coordination body with a budget of $500 million to complement it policymaking competencies.[19] In line with Israel's entrepreneurial approach to cyber, the government established a cyber-threat research cluster in the desert city of Beersheba which — echoing the genesis of major U.S. tech giants such as Google — involves a mix of government cyber experts, private sector, and research institutions.[20] Israel's Unit 8200, responsible for cyber operations, is the largest unit in the Israeli Defense Force. Netanyahu has adopted cybersecurity as a personal priority, and the aforementioned cyber bodies are institutionally linked to the prime minister's office. As early as 2011, Netanyahu publicly vowed to turn Israel into a "world cyber power." By early 2016, Israel had over 300 cybersecurity companies, exports of $6 billion, and 20 percent of the world's private investment in the cyber domain.[21]

As countries like Iran and Israel consolidate their gains as full-fledged cyber powers, other powers in the region are trying to catch up.

A Cyber Arms Race in the Gulf?

Since the 2012 Saudi Aramco attack, Iran and Saudi Arabia" have been lobbing digital artillery fire at each other in a simmering conflict"[22] that reached its preliminary climax with the GCC fallout over the Qatar crisis in June 2017. According to Qatar, hackers using United Arab Emirates-based devices breached the government's Qatar News Agency website to place fake comments attributed to Qatar's Emir that contained controversial remarks on Iran and other diplomatically sensitive regional issues. The breach, in which the UAE government denied involvement, quickly spiraled into the ongoing boycott of Qatar by its fellow GCC members Saudi Arabia, UAE, and Bahrain, as well as Egypt. Embarrassing emails from the account of the Emirati ambassador to the United States leaked shortly after, suggesting Qatari retaliation, although Qatar has denied any involvement.[23] The figures below, displaying instances of publicly known state-sponsored cyber operations collected by the Council on Foreign Relations, show that for the time being, the cyber arms race is above all a matter between Iran, Israel, and the GCC states, in which Saudi Arabia has a clear disadvantage.

15 Council of Foreign Relations, "Cyber Operations Tracker."

16 Ibid.

17 Kirk Soluk, "DDoS and Geopolitics: Attack Analysis in the Context of the Israeli-Hamas Conflict," Arbor Networks Report, August 2014.

18 Jeff Moskowitz, "Cyberattack Tied to Hezbollah Ups the Ante for Israel's Digital Defenses," Christian Science Monitor, June 15, 2015.

19 Israel Ministry of Foreign Affairs, "Cabinet Approves Establishment of National Cyber Authority," February 15, 2015.

20 Segal, 2017, p. 19-20.

21 Adam Segal, "The Middle East's Quietly Rising Cyber Super Power," Defense One, January 27, 2016.

22 Tim Johnson, "As U.S. Issues Warning to Iran, Persian Gulf Cyberwar Takes on New Meaning," McClatchy, February 1, 2017.

23 ABC News, "In the Persian Gulf, Computer Hacking Now a Cross-border Fear," ABC News," September 12, 2017.

Publicly Known State-Sponsored Cyber Operations in the MENA 2010–2017[24]

Country	Sponsored Attack	Victim of Attack
Iran	19	18
Israel	5	11
Saudi Arabia	0	16
United Arab Emirates	1	6
Syria	0	8
Turkey	0	6
Qatar	0	4
Lebanon	0	4
Iraq	0	3
Bahrain	0	1
Jordan	0	4
Kuwait	0	3
Yemen	0	2
Morocco	0	2
Algeria	0	3
Tunisia	0	1
Egypt	0	4
Libya	0	2

The digital security challenge in an increasingly antagonistic Persian Gulf has induced small Gulf states such as the UAE, who pride themselves on their smart city networks but fear increased vulnerability, to build major cyber defense industries.[25] According to the Organization of Islamic Cooperation, "the region's dramatic strides toward digitization — expected to add over $800 billion to GDP and over 4 million jobs by 2020 — is making the Gulf a major target for fast evolving cyber threats." In addition, heavy dependence on oil and gas, including for the provision of fresh water, makes the Gulf and other MENA countries particularly vulnerable targets for cyber-attacks with a big humanitarian impact. While the Gulf struggles like other regions to build effective criminal deterrence against digital breaches, even harmonized laws would be ineffective against state-sponsored hacking.[26]

The attacks of the past few years have led to a notable activism among GCC states to build cybersecurity capabilities, institutions, and strategies. Aside from building their own capabilities, Saudi Arabia and other GCC states also have the resources to outsource cyber operations to world-class hackers. In 2013, the year following the Shamoon attack on Aramco, Saudi Arabia adopted its first National Information Security Strategy.[27] In February 2017, Riyadh inaugurated its National Cyber Security Center at the Ministry of the Interior as a national technical coordination center for cyber defense. The Saudi cybersecurity market is projected to grow nearly 60 percent to $3.48 billion by 2019.[28] Similarly, the UAE established the Abu Dhabi-based National Electronic Security Authority in August 2012 and in 2017, adopted a Dubai Cyber Security Strategy.[29] Qatar's inter-ministerial cyber coordination body, the National Cyber Security Committee established the country's National Cyber Security Strategy in 2013.[30]

Tehran's considerable investments in developing its technological base and manpower suggest it will not stay behind Israel for long. Iran is using cyberspace to develop and deploy asymmetric tools against the United States and its own regional rivals in Israel and the Gulf. For Tehran, cyber-attacks square neatly with its expansive regional reach by means of proxy warfare. Conventional proxy warfare on the battlefields in Syria and Yemen bear great financial and human cost and are caught in a stand-off. Despite the different defense instruments at its disposal, it is at least doubtful to which degree Iran's conventional military would be able to compete with its regional and global rivals on the battlefield. Its cyber capabilities, by contrast, fare clearly favorably in regional comparison. Cyber-attacks allow Iran "to strike at adversaries globally, instantaneously, and on a sustained basis, and to potentially achieve strategic effects in ways it cannot in the physical domain," writes cyber expert Michael Eisenstadt.[31]

24 Number of publicly known, state-sponsored cyber activity in which the perpetrator is suspected to be affiliated with a nation-state in pursuit of its foreign policy. The figures exclude non-state actors such as hacktivists where no direct link to a government can be established. Source: Council on Foreign Relations, "Cyber Operations Tracker."

25 See for example, Marios-Panagiotis Efthymiopoulos, "Cybersecurity in Smart Cities: The Case for Dubai," *Journal of Innovation and Entrepreneurship*, February 27, 2016.

26 Maxey, op cit.

27 Saudi Arabia Ministry of Communications and Information Technology, "Developing National Information Security Strategy for the Kingdom of Saudi Arabia," Draft 7.

28 "Saudi Cybersecurity Market to Top $3.4bn," Trade Arabia, March 2, 2016.

29 Dale Benton, "Dubai Cyber Security Strategy Launched to Improve Data Security," *Middle East Business Review*, June 1, 2017.

30 State of Qatar, Ministry of Transport and Communications, "National Cyber Security Strategy."

31 Michael Eisenstadt, "Cyber: Iran's Weapon of Choice," The Cipher Brief, January 29, 2017.

If Iran's reliance on proxy agents[32] to conduct military operations on its behalf has made direct attribution to the Iranian leadership difficult, this is even more the case in cyberspace, as the degree of control over a hacker group is opaque and may quickly change as time passes. Iran is believed to have lent support to Cyber Hezbollah, the Syrian Electronic Army, the Yemen Cyber Army, and Hamas. Although the degree of control exercised by Iran's political leadership over intelligence agencies and, in turn, hired hackers is opaque, experts esteem that cyber-attacks on Iran's political rivals count on at least tacit approval from the regime.[33] As Michael Sulmeyer argues, Iran's heavy reliance on proxies, while aiding to dilute attribution, bears a number of risks. Proxies' interests may differ, or even conflict with those of their state sponsors, and they may be more inclined to absorb the risks of collateral damage. They may also care less than their sponsors about concealing their affiliation, thereby raising the risk to the state sponsor of tracking, retaliation, and escalation.[34] Finally, unlike transfers of guns or explosives to proxies that require regular fresh supplies, transferring cyber resources and tools to proxies once effectively removes those tools and technologies from state control. This in turn opens up the possibility that proxies may have less incentive to toe the line, that they may become independent from their state sponsors, or even use the tools obtained against the sponsor. In other words, if controlling proxies is a challenge in physical warfare, exerting such control will be even harder for state sponsors in the cyber realm.

> ***"Cyber-attacks square neatly with Tehran's expansive regional reach by means of proxy warfare."***

The possibility of escalating MENA antagonisms by means of cyber-attacks is further complicated by the fact that not only states — directly or via the hacker armies they may hire — but also autonomous non-state actors are using cyber-attacks and digital warfare more broadly to advance their aims. The spread of jihadist ideology and propaganda, recruitment and training materials, and encrypted communication via the Internet has long allowed transnational violent extremist groups to reach a global audience. As the self-proclaimed Islamic State group loses its territorial grip, its "social media empire" remains.[35] In fact, with the retreat on the physical battlefield, the group's geopolitical reach via cyber channels is likely to experience a new boost. An April 2013 hack by the Syrian Electronic Army (SEA), a group of hackers backing Bashar al-Assad, sent fake tweets on a prospective bomb attack on President Obama from the Associated Press' twitter account, leading to a plunge in the U.S. stock market. SEA also attacked other key Western news outlets including CBS, the BBC, *The Washington Post*, and the Onion, in retaliation for what it called one-sided coverage of the Syrian civil war.[36] A 2015 attack on France's TV5 Monde ascribed to ISIS is another display of the growing capability of Middle Eastern non-state cyber-attackers. However, while groups such as ISIS seek to build up offensive capabilities, experts say these do not yet get anywhere close to the capabilities and threats posed by state-sponsored hacking. In a similar vein, in late 2015 U.S. Deputy Director of Defense Robert Work stated, "terrorist groups, including ISIL, experiment with hacking which could serve as the foundation for developing more advanced capabilities. Terrorist sympathizers conduct low-level cyber-attacks on behalf of terrorist groups and attract attention of the media, which might exaggerate the capabilities and threat posed by these actors."[37]

Accelerating Destabilization

In some instances, Middle Eastern cyber proliferation has been part of the response to prolonged tensions and interstate conflict in the Middle East. The regional alienation of Iran, proxy wars in Syria, Yemen, and Libya, and the persistent enmity between Israel and its neighbors were all instrumental in driving the

32 See also Kristina Kausch, "Proxy Agents: State and Non-state Alliances in the Middle East," *The Frailty of Authority. Borders, Non-state Actors and Power Vacuums in a Changing Middle East*, Rome: Edizioni Nuova Cultura, 2016.

33 Michael Sulmeyer, "Cyberspace: A Growing Domain for Iranian Disruption," *Deterring Iran After the Nuclear Deal*, Center for Strategic and International Studies: Washington, DC, March 2017.

34 Ibid.

35 Bennett Seftel, "ISIS `Caliphate´ Fades but Social Media Empire Remains," The Cipher Brief, September 28, 2017.

36 Segal, 2017, p. 16-17.

37 Deputy Secretary of Defense Robert O. Work, "Opening Statement Before the House Armed Services Committee," September 30, 2015.

regional cyber build-up and the determination to use them against political rivals of the state (at home and) abroad.[38]

At the same time, the political use of cyber tools works as a powerful accelerator of geopolitical confrontation in the Middle East, with the potential to take regional destabilization to a new level. Existing political tensions and conflicts in the MENA region gain an additional arena for much faster escalation. In many ways, this has already happened. The Qatar episode has shown how ripe the Gulf's political fragility is for exploitation by means of cyber operations. Just one targeted hack into an already tense regional set-up can single-handedly put at risk both the Gulf security order on which U.S. Middle East policy has rested, and the continuity of the U.S.-led Global Coalition to Defeat ISIS. As fronts harden after five months of stand-off, a permanent low-level confrontation looks increasingly likely. Without a unified GCC, countering Iranian influence in the region will be difficult. Western observers fear that the crisis creates inroads for Iran and others into what has so far been a solidly pro-Western political and security arrangement in the Gulf.[39] The rise in capabilities and awareness of the geopolitical potential of cyber-attacks has expanded the intra-Arab rift, already manifest on conventional battlefields in Yemen, Syria, and Libya, and on the digital level as well.

> *"Overtly aggressive operations that cross a red line could lead to a full unraveling of regional relations."*

Among the immediate destabilizing effects is the impact Iranian (real or suspected) cyber prowess could have on the Joint Comprehensive Plan of Action (JCPOA) and Tehran's relations with global powers more broadly. Iran's continued cyber-attacks on U.S. political and corporate targets will likely influence U.S. policy circles in their overall evaluation of the relationship with Tehran, especially Congressional support for the JCPOA. If Iran reduces the scope of attacks on U.S. targets and instead focuses on less overtly aggressive operations against regional adversaries, the latter will look to the U.S. for support.

At the same time, regional adversaries may try to take advantage of the difficulties of firm attribution to justify desired offensive action against each other and/or draw support from allies abroad. For example, with Iran branded as an aggressive regional rogue, false-flag cyber operations seem like a golden opportunity for Iran's rivals to gain geopolitical advantage in relations with the Trump administration. A version of the Shamoon virus that hit Saudi Aramco in 2012 attacked Saudi government computers in November 2016, this time displaying a picture of the drowned Syrian toddler Aylan Kurdi. Some experts have suggested that this attack might have been a false-flag operation to derail the JCPOA.[40]

Overtly aggressive operations that cross a red line in a region where nerves already lay blank, for example the deployment of a powerful cyber weapon with effects reaching into the physical world by Iran, could lead to a full unraveling of regional relations. Such an escalation could affect not only cyber fronts but also the Iranian nuclear dispute, all proxy battlefronts of the Middle East in Syria, Yemen and Libya, and possibly open up new physical frontlines. Cyber experts point out that in the range between constant low-level attacks and big cyber weapons, destructive attacks of the Shamoon kind are going to increase in frequency and destructive power as more and more states acquire offensive cyber capabilities. But even in the absence of large-scale attacks, a continuation or increase of the current "cyber artillery" in the region will likely contribute to a further hardening of fronts between Iran on the one side and Saudi Arabia and Israel on the other. Riyadh's sense of siege would reach new heights, building up to a showdown further down the road. One way or another, Iran's status as a growing power in cyberspace means that the political rivalries and long-standing tensions of the Gulf and the Middle East more generally are only poised to worsen.[41]

38 HIS Markit, *Expect Middle East Conflicts to Have Increasing Cyber Effect*, April 21, 2015.

39 Kristian Coates Ulrichsen, quoted in Kaitlin Lavinder, "Trump and Kuwait Emir Hint at End to Gulf Crisis," The Cipher Brief, September 7, 2017.

40 Michael Riley, Interveiw with Bloomerberg Technology, "Destructive Hacks Strike Saudi Arabia, Posing Challenge to Trump," Bloomberg, December 1, 2016.

41 Michael Eisenstadt, "Cyber: Iran's Weapon of Choice," The Cipher Brief, January 29, 2017.

In addition to the risk of further regional escalation, what is now mostly an inner-Gulf confrontation could develop into a larger block confrontation as adversaries try to drag in other actors for support. Ongoing efforts by regional powers Saudi Arabia, Egypt, Qatar, and Iran to build relationships with China, Japan, India, and Russia to hedge against uncertainty surrounding continued engagement by the United States and Europe in the region appear to be accelerated by the Qatar crisis, leading to important shifts the Middle Eastern relationship puzzle.[42] This is already becoming a reality as an isolated Doha turns to Iran, Turkey, and Russia, and the rest of the GCC to the United States and Israel. Qatar has been able to make up for the economic damage caused by the GCC blockade by switching its main trade partner from the UAE to Oman and reaching out to Iran and Turkey. The result of the blockade is a lasting split in the Gulf that strengthens Iran and pins a group of assertive powers with hegemonial ambitions — Iran, Russia, and Turkey — against the rest. The Gulf split has been in the making for years and is grounded in reasons that pre-date MENA cyber proliferation. Yet, it has been duly noted in the Gulf and beyond that it was a cyber-attack that provided the trigger to turn simmering hostilities into a full-fledged diplomatic escalation.

In some instances, the rise of cyber as additional arena for MENA geopolitics may bear some potential to help avoid or ease conflict. For example, states may choose to launch cyber operations in order to avoid conventional military attacks on the ground. The Israeli–U.S. Stuxnet attack may have contributed to avoiding an Israeli preventive strike on Iran. However, such substitutive effects are undone to the degree states vow to retaliate to cyber-attacks not only in kind but by all means available. Benjamin Netanyahu has stated Israel will not shy away from using military force to retaliate after a massive cyber-attack, to "both treat the attack and treat the attacker."[43] Executive Order 13694 signed by President Obama in April 2015 gives the U.S. government the ability to respond to malicious cyber activities outside of the cyber realm.[44]

> *"A hesitant U.S. response would give Tehran time and room for maneuvers to continue and succeed"*

A possible positive windfall of the GCC's confrontational surge with Iran, including in the cyber domain, is that it seems to favor a degree of pragmatic rapprochement of some of the GCC states with Israel, Iran's regional rival and the region's first cyber and conventional military power. Bahrain, on the front line as a small Shia majority state, has recently adopted a notably friendly public discourse on Israel. Israeli diplomats maintain that Bahrain's shifting stance is unlikely to have gone ahead without the approval of Saudi Arabia, and unconfirmed reports of an upcoming formal Saudi–Israeli rapproachment abound. The fear that a possible disengagement of the United States in Syria after the territorial defeat of ISIS will leave the field to Iran and Russia may further contribute to this informal rapprochement.

A Closing Window to Show Readiness

The increasing use of cyber-attacks for geopolitical aims may accelerate the unraveling of an already unstable, war-ridden Middle East. Cyber-geopolitics will shape the relationship between Iran and its neighbors; and allies of both sides, in particular the United States, are bound to play a central role in this confrontation out of the limelight. The United States is the world's leading cyber power, but it may never be as strong again in cyberspace as it is today. As much of the cyber operations will be calculated in relation to the odds of retaliation and to the impact they may have on the target's alliances, it will be crucial to set clear limits and ensure effective deterrence while Iran's capabilities remain limited.

Although it is unclear whether Iran would retaliate to cyber-attacks by military means, it has until now responded in kind, and the broad dependency of the U.S. economy on relatively vulnerable computer

42 ControlRisks: Middle East Risk Watch, Issue 6, March 2017.

43 Adam Segal, "The Middle East's Quietly Rising Cyber Super Power," Defense One, January 27, 2016.

44 White House, "Executive Order: Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," December 29, 2016.

networks has given it many opportunities to do so. According to some experts, given U.S. cyber vulnerability, the best means to deter Iran in the cyber domain is to threaten military action. Yet, like with all deterrence, the value of such threats depends on their credibility. Eisenstadt writes: "Washington's embrace of Stuxnet to avert an Israeli military strike on Iran's nuclear program probably reinforced the perception that it was reluctant to challenge Tehran in the physical domain. Paradoxically, this milestone use of offensive cyber may have inadvertently undermined cyber deterrence."[45] Iran is well aware of the damaging effects of direct attacks on U.S. targets on the global economy, and of the U.S. ability to retaliate to them, so it might exercise constraint on that front. However, it could place its bets instead on the possibility that the United States will be wary of getting involved in retaliatory measures on behalf of its Gulf allies. A hesitant, muffled U.S. response to cyber aggression overseas would give Tehran time and room for maneuvers to continue and succeed, effectively deterring the United States' and its allies' ability to defend their interests."[46]

Deterrence works by convincing one's adversary that the costs of conducting an attack outweigh potential benefits. To deter Iranian cyber-attacks, the United States and its Middle Eastern allies will need to stay tuned to Tehran's political sensitivities and priorities to ensure both deterrents and retaliatory measures produce the desired effect.[47] The biggest risk for Western powers is to leave any doubt about their readiness to retaliate or to support their allies against any actors' cyber aggressions. If Iran, for example, perceives that its cyber-attacks have no consequences, escalation is a foregone conclusion. A united front against disruptive and destructive Iranian cyber prowess, including a systematic readiness to publicly expose and attribute those actions, is key.[48] As actors around the world begin at an alarming pace to grasp the opportunities offered by conducting geopolitical operations in cyberspace, the window for showing this readiness is small and closing.

45 Michael Eisenstadt, "Cyber: Iran's Weapon of Choice," The Cipher Brief, January 29, 2017.

46 Admiral Michael S. Rogers, Commander, United States Cyber Command, "Statement Before the Senate Committee on Armed Services," September 29, 2015.

47 Sulmeyer, op. cit.

48 Ibid.

The views expressed in GMF publications and commentary are the views of the author alone.

About the Author

Kristina Kausch joined The German Marshall Fund of the United States' (GMF) Brussels office in September 2016. She comes to GMF as part of a two-year fellowship supported by the European Commission under the Marie Curie program.

The author would like to thank Cornelius Adebahr, Joost Hiltermann, Amy Studdart, Guillaume Xavier-Bender, and John Alexander for their excellent comments on an earlier draft of this article; and thanks to Amal Bourhrous for the helpful research assistance.

About GMF

The German Marshall Fund of the United States (GMF) strengthens transatlantic cooperation on regional, national, and global challenges and opportunities in the spirit of the Marshall Plan. GMF does this by supporting individuals and institutions working in the transatlantic sphere, by convening leaders and members of the policy and business communities, by contributing research and analysis on transatlantic topics, and by providing exchange opportunities to foster renewed commitment to the transatlantic relationship. In addition, GMF supports a number of initiatives to strengthen democracies. Founded in 1972 as a non-partisan, non-profit organization through a gift from Germany as a permanent memorial to Marshall Plan assistance, GMF maintains a strong presence on both sides of the Atlantic. In addition to its headquarters in Washington, DC, GMF has offices in Berlin, Paris, Brussels, Belgrade, Ankara, Bucharest, and Warsaw. GMF also has smaller representations in Bratislava, Turin, and Stockholm.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 701306.

1744 R Street NW
Washington, DC 20009
T 1 202 683 2650 | F 1 202 265 1662 | E info@gmfus.org
http://www.gmfus.org/