CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES | Middle East Program

January 2014

GULF ANALYSIS PAPER

SUMMARY

The Gulf has become a flashpoint for cyber conflict. Cyberspace has become an arena for covert struggle, with the United States, Israel and other nations on one side, and Iran and Russia on the other. Iran has far outpaced the GCC states in developing its cyber capabilities, both for monitoring internal dissent and deploying hackers to disrupt or attack foreign targets. Several such attacks over the past two years were likely either directed or permitted by Iranian state authorities. Even if Iran holds back from offensive actions as nuclear talks progress, the growth in Iranian capabilities remains a potential security threat for other Gulf states. The GCC countries have begun to develop their defensive capabilities, but they will need to expand their defenses and collaborate more effectively to deter future threats. ■

Cybersecurity and Stability in the Gulf

By James Andrew Lewis[1]

"The Iranian attack on the Saudis was a real wake-up call in the region."

Unnamed senior U.S. official, *New York Times*, June 9, 2013

Cyberattack is a new tool of national power. It provides a means of coercion, influence, and warfare. The use of cyber techniques as intelligence tools dates back to the 1980s; cyberattack by militaries dates back to the 1990s.[2] Using cyber tools and techniques as an instrument of national power is the norm in the Gulf. The Gulf has become a flashpoint for cyber conflict given the high level of activity and the chance for miscalculation and escalation into conventional conflict.

The Gulf is unique in that the use of cyber techniques by governments for covert action is much more prevalent than in any region other than the Korean peninsula. The primary source of tension among Gulf states is the development by Iran of cyberattack capabilities that it has used and appears willing to use again. There is also a growing concern about Israeli cyber capabilities. This is an outgrowth of the larger disputes between Iran and Gulf Arab nations. Given the Gulf's strategic and economic significance, cyber attacks that damage oil production or escalate into physical conflict could have global consequences. The use of cyber tools and the expansion of cyber capabilities could change the balance of military power among regional states and undermine Gulf stability, particularly if the Gulf Cooperation Council (GCC) states do not expand their defenses in response to this new threat and find ways to better cooperate.

Three key incidents have focused the attention of Gulf states on cybersecurity. The first was the effect of social media and the Internet in the Arab uprisings of 2011 and the 2009 Iranian "Green Revolution." The Internet can amplify politi-

GULF ANALYSIS PAPERS

In conjunction with its Gulf Roundtable series, the CSIS Middle East Program issues periodic policy papers addressing key economic and security issues in the Gulf region. Launched in April 2007, the Gulf Roundtable series convenes monthly and assembles a diverse group of regional experts, policymakers, academics, and business leaders seeking to build a greater understanding of the complexities of the region and identify opportunities for constructive U.S. engagement. Topics for discussion include the role of Islamist movements in politics, the war on terror, democratization and the limits of civil society, the strategic importance of Gulf energy, media trends, trade liberalization, and prospects for regional integration. The roundtable defines the Gulf as the United Arab Emirates, Saudi Arabia, Oman, Qatar, Bahrain, Kuwait, Iraq, and Iran and is made possible in part through the generous support of the Embassy of the United Arab Emirates. ■

cal forces in ways that are difficult to predict or control. The second was the Stuxnet attacks launched against Iranian nuclear facilities in 2010. Stuxnet led to significant changes in Iranian policy, but it was not unique. Researchers around the world discovered significant malware programs—Stars, Duqu, Flame, Shamoon—used for espionage or attack against Gulf targets.[3] Finally, the 2012 attacks on Saudi Aramco and the Qatari firm RasGas, generally attributed to Iran, put most Gulf countries on notice of the new kind of risk they faced.

In response to increased Iranian capabilities, the United States has begun to work with partner nations in the Gulf to improve their cyber defense capabilities. But almost all current "cyber powers" play some role in the Gulf. Israel has a close and active interest in Iran, and Israeli sources report that Iran routinely probes Israel's networks for vulnerabilities. Russia has worked with Iran in ways we do not fully understand and has sought to work with GCC states as well. There are reports that North Korea and Iran may be collaborating in developing cyberattack tools.

The use of cyber techniques by governments in the Gulf for covert action is much more prevalent than in any region other than the Korean peninsula.

Nations' larger goals and interests determine how they use cyber techniques, guided by their strategies, experience, institutions, and tolerance for risk. It is not yet clear if, over time, the ability to acquire and employ cyber techniques will encourage states to be more assertive or confrontational. Access to the new cyber tools does not yet seem to have led countries to fundamentally change their policy objectives; intent better explains activity in cyberspace than does capability when it comes to conflict.

We can assess the relative strength of different Gulf states' cyber capabilities by looking at factors that predict those capabilities. These include institutions, strategies, and investments for cyber activities; the integration of cyber activities into existing military, intelligence, and diplomatic strategies; and the level of political attention given to cyber capabilities by national leaders, military commanders, or the heads of other ministries. Commitments and partnerships with other nations for cyber activities also predict relative strength.

Iran's Cyber Capabilities

Iran is far in the lead over the GCC states. Iran's trajectory in developing cyber capabilities is a good example of how a medium-sized government willing to commit a relatively small amount of resources can build cyber power. Iran sees cyberattack as another tool of its broader asymmetric warfare strategy for use against more powerful opponents.[4]

Iran's own experiences have given it a keen appreciation for the utility of cyber techniques as instruments of national power and tools for coercion and force. Iran's concern over cyber threats originated with its need to repress dissent, and its development of cyber power is a reaction to the vulnerabilities created by the Internet. During the 2009 "Green Revolution," Iranian security forces expanded their ability to monitor and disrupt online dissent as part of a broader crackdown on opposition activities. Iran's leaders fear the power of networks to unleash a more widespread popular uprising in Iran like those which toppled regimes in Tunisia and Egypt in 2011. Since then, Iranian security forces have expanded their ability to monitor and disrupt online dissent into an ability to use cyber techniques against other states, the most notorious example being the 2011 hack of the Netherlands Internet company DigiNotar, which allowed Iran to surreptitiously read Iranian dissidents' emails.[5]

Repeated foreign intrusions led to high-level attention to cybersecurity and the creation of a sophisticated organizational structure to manage cyber conflict. In 2011 Iran's Supreme Leader Ayatollah Ali Khamenei authorized the establishment of a new "Supreme Council of Cyberspace" to coordinate efforts for both offense and defense. Council members include senior officials from the security and intelligence services and the ministers of culture and communications. Iran has a comprehensive cybersecurity strategy that includes the creation of what it calls a "national information network" that could disconnect most of Iran from the global Internet. Several prominent Iranian securi-

Iran's concern over cyber threats originated with its need to repress dissent, and its development of cyber power is a reaction to the vulnerabilities created by the Internet.

ty officials have commented publicly on Iran's capabilities and the importance of cyberwarfare more broadly. Iran's Revolutionary Guard Corps (IRGC) Deputy Commander Abdollah Araghi said, "We have equipped ourselves with new tools since cyberwar in the cyberspace is more dangerous than physical war, and Iranian officials, especially the Supreme Leader of the Islamic Revolution have all cited this point, therefore we are prepared for soft and physical wars."[6] Interior Minister Mostafa Najjar has also said that "satellites and Facebook are the electronic means of a 'soft war' by the West to cause the Iranian family's collapse."[7]

Three Iranian military organizations have operational cyber roles: the IRGC, the Basij, and Iran's Passive Defense Organization. Iran held its first national cyber defense exercise in late October 2012. The Basij, a civilian paramilitary organization controlled by the IRGC, manages the Iranian "Cyber Army," which Basij leaders say has 120,000 volunteer hackers. The number is certainly an exaggeration, but the Basij uses its already close connections with universities and religious schools to recruit a proxy hacker force.

The Cyber Army is the likely source of a recent series of incidents aimed at Gulf energy companies, American banks, and Israel. The most important involved a major disruption involving the destruction of data on computers used by Saudi Aramco and RasGas. U.S. intelligence sources indicate that Iran was responsible for the attacks. The trigger for these incidents was most likely a cyberattack on Iran's major oil terminal at Kharg Island. Iran appears to have cleverly modified cybercrime malware for the attack. All the data on 30,000 Aramco computers was erased, and the malware may have infected (though it did not damage) refinery control systems. The Aramco incident, while not as sophisticated as Stuxnet, was second only to Stuxnet as a disruptive cyberattack and showed the progress of Iranian capabilities.

At the same time that the Aramco incident took place, there were massive "denial of service" attacks against U.S. banks. The likely trigger for the attacks on U.S. banks, which continue to this day, was the imposition of new sanctions by the U.S. Congress on Iran.[8] Denial of service is more like an online demonstration or protest than an attack; the target network is flooded with spurious traffic that causes it to fail, but the perpetrator does not gain access to the target network. The Iranian efforts follow the Russian pattern of using proxy hackers for political coercion, as when Russian hackers used denial of service attacks against Estonia in 2007. The harassment of American banks, however, was many times larger than the attacks on Estonia and at first overwhelmed the banks' ability to respond. Attacks of this size require computing resources that, in a country where the Internet is tightly controlled, indicate government approval, if not direction, was involved. There are some reports that Iran has turned to outside help in developing malware, either to Russian cyber criminals (who are among the best in the world) or, paralleling its proliferation activities, to North Korea.

It is too early to tell if progress in negotiations between Iran and Western countries on its nuclear program decreases the risk of a cyber incident. Iran is likely to be on its best behavior during the negotiations to avoid damaging any progress toward sanctions relief (although it is possible that Iranian opponents to the negotiations could use a cyber incident in an effort to derail the talks). Even if there is progress, the growth in Iranian capabilities remains a potential security threat for GCC states.

Cyber Capabilities among the GCC States

The combination of the attacks on Aramco and the banks is best seen as a test by Iran of its new capabilities and of the U.S. and GCC reactions to them. In response to Iran's growing capabilities and cyber activism, Gulf nations have begun to increase their defensive capabilities. A series of politically motivated incidents targeting Gulf media outlets, attributed to the Syrian Electronic Army and to the hacker group Anonymous (although this could be anyone), have increased Gulf states' concerns. The United

The combination of the attacks on Aramco and the banks is best seen as a test by Iran of its new capabilities and of the U.S. and GCC reactions to them.

Arab Emirates (UAE) has had a cyber capability for some time, largely provided by outside contractors, but in 2012 it introduced cybercrime legislation and established a new national authority for cybersecurity, the National Electronic Security Authority (NESA). NESA is an independent agency linked to the UAE Supreme National Security Council, and it was created through a special federal decree issued by the UAE's president. NESA's mandate is to defend against attacks on military and critical infrastructure and oversee cybersecurity across all government agencies.

The cybersecurity concerns of GCC states mirror their broader strategic objectives: preserving domestic political control, containing Iranian ambitions (with the United States as a counterbalance), and maintaining an uneasy balance between cooperation and competition with their neighbors. The United States has encouraged and assisted GCC states in improving their cyber defenses. This includes some direct assistance (in the form of advice and technology) and through the services of U.S. contractors. Qatar began its own cybersecurity initiative in February 2013, with Saudi Arabia and Bahrain.[9] Kuwait reportedly entered into a $1 billion program on physical security and cybersecurity with the United Kingdom.[10] Bahrain, after experiencing annoyance attacks attributed to Anonymous, is paying greater attention to cybersecurity, working with Western contractors; whether this will translate into tangible improvements remains to be seen. Bahrain also arrested hackers from the "February 14 Revolution Youth Coalition" and accused them of having ties to Iran, reflecting the expanded use of cybersecurity to control political dissent across the region.[11]

There are also efforts to strengthen the GCC's cooperation in cybersecurity. These have not yet produced tangible results, but if the GCC were to become a hub for sharing threat and mitigation information among its members, it would significantly improve cyber defenses. Gulf countries have something of an advantage in developing cyber defenses given the high degree of control already exercised by governments over national telecommunications companies. Cooperating with the United States and others in the face of Iranian belligerence and committing the resources to invest in cybersecurity efforts would enable Gulf countries to build on the advantage of being well-resourced and exercising a high degree of control over their national telecommunications networks.

External Actors

The Internet eliminates distance and provides a new way for outside nations to intervene in the Gulf region. The primary focus has been intelligence collection, but nations have also used cyber techniques for political influence and for covert action. Iran is a hard target for intelligence collection. Western nations, with the United States foremost among them, have been quick to add cyber capabilities to the intelligence collection assets they already deploy to monitor Iran. U.S. interests are aimed at slowing Iran's nuclear program and improving the cyber defenses of friendly nations in order to reduce risks to regional stability.

Media accounts ascribe various covert actions against Iranian targets to the United States (the most famous being Stuxnet, identified in the press as part of a larger covert cyber operation named "Olympic Games"). Israel has been the target of sustained efforts by Iran to hack into and disrupt Israeli networks, and while Iran has had only limited success, Israel has itself not been shy about using its advanced cyber capabilities for purposes of espionage and, perhaps, attack. China does not seem to have played a major role in the Gulf (there is no public evidence of support for Iran from China for malicious cyber activity), although given the pattern of China's activities in the rest of the world, it is reasonable to speculate that it has engaged in espionage against Gulf energy companies to gather commercially valuable information.

Russia's calculations may be somewhat different, as the activity in the Gulf appears to have served as a vehicle for demonstrating larger Russian concerns about the Internet. Russia, for example, supported the International Telecommunications Union (ITU) when it hired a Russian firm with links to the Federal Security Service (FSB) to in-

vestigate cybersecurity problems in the Gulf. This ITU activity was unprecedented. It could simply be coincidence that these efforts act to reinforce other Russian efforts to place the ITU at the center of cybersecurity—putting the Internet, like global telephone communications, under its purview. Revelations about Flame and Stuxnet served, perhaps fortuitously, the larger Russian political agenda on Internet governance, which seeks to establish tighter political control over uses of the Internet and to undercut U.S. "hegemony." Gulf states are sympathetic to Russian views on controlling content and supported Russian internet governance ideas at the World Conference on International Telecommunications held in Dubai in December 2012. Cybersecurity provides a low-cost means for Russia to play a role in the Gulf.

The Future of Cybersecurity in the Gulf

Cyberspace has become an arena for covert struggle, with the United States, Israel and the GCC on one side, and Iran and Russia on the other. Iran's nuclear program is a magnet for cyber espionage, and Iran itself has discovered the value of cyberattack. This covert struggle spills over into Iran's regional neighbors. Iran and external actors like the United States, Israel, and Russia will continue to use cyber techniques for covert activities to achieve national goals. In the Gulf as in the rest of the world, cyberattack provides a new tool for nations to use in existing disputes.

The variables that affect the likelihood of future cyberattack are the state of relations between Iran, its neighbors, and important external actors; the perceived likelihood of attribution; and the quality of Gulf nations' cyber defenses. With the global spotlight on the Gulf and Iran, the risk of a major cyberattack in the Gulf may actually be reduced (although by how much we cannot say—certainly not enough that GCC states can afford not to take their defenses seriously). Part of Iran's calculation in using cyber tools is the probability of detection, attribution and retribution (political or military, covert or overt). Since the likelihood of attribution has increased—and it would be beneficial to ensure Iranian awareness of this—Iran may be less interested in using cyberattacks. This assumes, of course that the Iranians believe they will be detected, that they care about the foreign reaction, and that they will conclude that the risks of cyberattacks outweigh the benefits.

Collective defense among Gulf states remains problematic, as it does in other security areas. The United States can play a brokering role. States reluctant to cooperate directly with each other can use bilateral cooperation with the United States in cybersecurity as an indirect mechanism for coordination. This is not an ideal situation, but it is better than uncoordinated individual efforts.

If the Gulf did not face larger security problems, cybersecurity would be a much smaller issue, perhaps limited to financial crime and commercial espionage against oil companies. As it is, with the increased attention to cybersecurity and the increased awareness of Iranian activities (and Israeli capabilities), all sides in the cyber contest are now wary and increasingly prepared. At the moment, Iran leads the Gulf region when it comes to cyber capabilities, although it faces powerful external antagonists. To raise the costs for Iran of using cyber weapons, the GCC states will need to dramatically strengthen their own cyber capabilities and expand their existing security partnerships to address cybersecurity. A failure to do so will raise the risk of cyberattacks that could trigger wider regional conflict. ■

About the Author

James Andrew Lewis *is a senior fellow and director of the Strategic Technologies Program at CSIS, where he writes on technology, security, and the international economy. Before joining CSIS, he worked at the Departments of State and Commerce as a Foreign Service officer and as a member of the Senior Executive Service. His government experience includes work on a range of politico-military and intelligence issues. He was the rapporteur for both the 2010 and 2013 UN Group of Government Experts on Information Security. Lewis has authored numerous publications since coming to CSIS, publishing a series of reports and essays exploring the relationship between technology and national power. He is an internationally recognized expert on technology and strategy whose work includes the report* Securing Cyberspace for the 44th Presidency *(CSIS, 2008). Lewis led a long-running track II dialogue on cybersecurity with China. His remarks appear frequently in the media, and he has testified numerous times before Congress. His current research examines international security and governance in cyberspace and the effect of the Internet on politics. Lewis received his Ph.D. from the University of Chicago.*

Notes

1. I would like to thank Eneken Tikk-Ringas for her very helpful comments.

2. Clifford Stoll's *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage* (New York: Doubleday, 1989) details Soviet cyber espionage in the 1980s. U.S. officials have described the use of primitive cyber attacks against Serbia in the 1990s.

3. Stars is a virus Iran claims to have discovered attacking its networks in 2011. Duqu is an espionage program that collects information from infected computers. Mahdi, designed for remote listening and control, affected networks in Iran and four other Middle Eastern countries in 2012. Shamoon wiped data from 30,000 computers belonging to Saudi Aramco in 2012. Flame can capture a broad array of information and has affected computers in Iran, Israel, Lebanon, Sudan, Egypt, Syria, and Saudi Arabia.

4. The motives and actors in the murder of a senior IRGC official remain unclear; the IRGC itself has said it was not an "assassination" and the investigation of the incident continues. "Iran Denies Cyber War Commander Mojtaba Ahmadi was Assassinated," *IB Times UK*, October 3, 2013, http://iranian.com/posts/view/post/21922.

5. "Fake DigiNotar web certificate risk to Iranians," BBC, September 5, 2011, http://www.bbc.co.uk/news/technology-14789763.

6. Ahmad Rezaie, "General Araghi: Iran is Ready For Any Hard and Soft Wars," *Kabir News*, September 25, 2012, http://kabirnews.com/general-araghi-irgc-is-ready-for-any-hard-and-soft-wars/3287/.

7. "Iran government develops 'National Internet' to combat international Internet's impact," Reporters Without Borders, August 3, 2011, http://en.rsf.org/iran-government-develops-national-03-08-2011,40738.html.

8. Ellen Nakashima, "Iran blamed for cyber attacks on U.S. banks and companies," *Washington Post*, September 21, 2012, http://articles.washingtonpost.com/2012-09-21/world/35497878_1_web-sites-quds-force-cyberattacks.

9. Joseph Varghese, "Ministry planning cyber security system for Qatar," *Gulf Times*, February 12, 2013, http://www.gulf-times.com/qatar/178/details/341898/ministry-planning-cyber-security-system-for-qatar.

10. "UK and Kuwait to announce security partnership," BBC, November 28, 2012, http://www.bbc.co.uk/news/uk-20530427.

11. "Bahrain arrests 'Iran-linked' cyber group," *Al Jazeera*, June 13, 2013, http://www.aljazeera.com/news/middleeast/2013/06/201361393933204365.html.

CSIS MIDDLE EAST PROGRAM

Jon B. Alterman
Director and Zbigniew Brzezinski Chair in Global Security and Geostrategy

Haim Malka
Deputy Director and Senior Fellow

Carolyn Barnett
Research Fellow

Rebecka Shirazi
Program Coordinator and Research Associate

Jason Mullins
Research Assistant

Breanna Thompson
Intern

Please visit our website at **www.csis.org/mideast** to learn more about the program's work.