Cybersecurity Strategies of Gulf Cooperation Council Economies

By: Nir Kshetri

Kshetri, Nir (2016)."Cybersecurity Strategies of Gulf Cooperation Council Economies," *Georgetown Journal of International Affairs,* March 15, 2016, https://www.georgetownjournalofinternationalaffairs.org/online-edition/cybersecurity-strategies-of-gulf-cooperation-council-economies

Made available courtesy of *The Georgetown Journal of International Affairs*: https://www.georgetownjournalofinternationalaffairs.org/

*****© *Georgetown Journal of International Affairs*. Reprinted with permission. No further reproduction is authorized without written permission from *Georgetown Journal of International Affairs*. This version of the document is not the version of record. Figures and/or pictures may be missing from this format of the document. *****

Abstract:

The countries that comprise the Cooperation Council for the Arab States of the Gulf (GCC)—Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates (UAE)—have become attractive cyber-attack targets thanks to their oil-fueled prosperity, liquid capital, and geopolitical and cultural positions. These cyber-threats and the GCC's responses, resources, and capabilities have significant global implications. For example, the 2012 attacks on Saudi Arabia's state-owned oil company, Aramco, had significant influence on the Pentagon's decision to drastically expand its own cybersecurity (CS) force in the U.S. Cyber Command.

Keywords: cybersecurity | Cooperation Council for the Arab States of the Gulf (GCC) | cybercrime

Article:

The countries that comprise the Cooperation Council for the Arab States of the Gulf (GCC)—Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates (UAE)—have become attractive cyber-attack targets thanks to their oil-fueled prosperity, liquid capital, and geopolitical and cultural positions. These cyber-threats and the GCC's responses, resources, and capabilities have significant global implications. For example, the 2012 attacks on Saudi Arabia's state-owned oil company, Aramco, had significant influence on the Pentagon's decision to drastically expand its own cybersecurity (CS) force in the U.S. Cyber Command.

This and numerous other high-profile attacks have intensified efforts by GCC nations to strengthen CS, with many placing it at the forefront of their security agendas. Qatar, for one, has made CS one of its three priority challenges, along with energy and water security, and has also established a Cybercrime Investigation Center and an Information Security Center. The UAE, for another, announced last year that it would double its security spending over the next ten years, with the majority going to CS. These regulations have been shaped by a variety of factors, including Sharia principles, a drive toward economic modernization, and an increasingly international geopolitical orientation.

The United States' and other Western nations' interest in the GCC countries' CS initiatives also is growing as their services become increasingly important in intelligence gathering and information sharing. This is particularly true for hot-button issues in the Middle East, including Iranian arms developments. Private CS firms are also gaining interest because of the new market opportunities opening up in the wake of the aforementioned recent cyber-attacks.

Threats, Vulnerabilities, Risks, and Challenges

The GCC economies' efforts to improve CS are significantly hindered by a lack of resources, experience, and training in their criminal justice and law enforcement systems. Saudi Arabia serves as an illustrative case in point. In order to effectively protect itself, based on the size and structure of its economy, Saudi Arabia would need to train 3,000 CS experts and provide basic skills instruction to tens of thousands more.[1] Similarly, a cybercrime seminar organized by Oman's state-run Informational Technology Authority (ITA) recommended that several judges and the much of the Royal Oman Police would have to be trained in cybercrime cases.

Despite these capacity-building challenges, the GCC economies' attempts to modernize their natural gas and petrochemical industries involve significant investment in computing platforms, making CS a key security concern. The attacks on Saudi Arabia's Aramco, which have been attributed to a virus called Shamoon, wiped out the hard drives of 30,000 computers—85 percent of the oil giant's devices—and shut down the company's business for two weeks at a cost of over U.S. $15 million. Several months later, the Shamoon malware attacked again in an attempt to disrupt international supply flows. Since Aramco is a state-owned company, these cyber-attacks can arguably be considered attacks against Saudi Arabia itself. This problem extends beyond Saudi Arabia: the same month Shamoon was attacked the second time, Qatar's liquid natural gas company, RasGas, experienced cyber-attacks associated with the same virus, shutting down its website and computer servers. According to U.S. officials and Middle Eastern private sources alike have attributed the attacks on Aramco and RasGas on the Iranian government.[2] The attacks took place shortly after Saudi Arabia expressed its intention to increase oil production to counter any supply problems caused by sanctions on Iran.

Regulations and Strategies

The GCC states contain a number of free zones with more developed guidelines and regulations for data protection. For instance, the Dubai International Financial Center (DIFC) has its own legal system and courts with jurisdiction over corporate, commercial, civil, employment, and trust matters. Another free zone is Dubai Healthcare City (DHC), which provides medical services. Likewise, the Qatar Financial Center (QFC), which was established to attract international financial services, follows legal structure based on English common law. These free zones have enacted data protection laws modeled after the European Union's data protection directive to regulate the processing, storage, and transfer of personal data.

Understanding why non-free zones have such lax regulations, however, necessitates understanding Sharia law's effect on privacy. It is against Sharia principles to invade an individual's privacy and disclose secrets without his or her permission, especially if it is not in the public interest to do so. Thus, constitutions in GCC countries tend to hold an individual's right to privacy sacred. The Saudi Arabian constitution, for example, guarantees the privacy of telephonic, telegraphic, postal and other forms of communications, and prohibits surveillance or eavesdropping on them. The Saudi 2007 Anti-Cyber Crime Law created civil and criminal sanctions for violations of personal data privacy, including the interception of data transmitted through information networks and the unauthorized access of financial data.

Another complication is that legal and law-enforcement structures within GCC countries have been designed primarily to tackle internal threats against their rulers. In 2012, Reporters Without Borders named both Bahrain and Saudi Arabia "The Enemies of the Internet." According to its report, these countries "combine often drastic content filtering with access restrictions, tracking of cyber-dissidents and online propaganda." Observers have noted that Saudi Arabia's crackdown against online activists has reached "extremely worrying levels." Human rights defenders face threats, harassment, arbitrary detention, imprisonment, torture, and fabricated judicial proceedings levied against them. In July 2014, Saudi human rights activist Waleed Abulkhair was sentenced to 15 years in prison, fined a large sum of money, and banned from leaving the country for 30 years after making comments on social media and remarks to the news media about the country's miserable human rights record. In June 2013, the Saudi government banned Viber, an app that lets users call, send messages, and share photos with each other. In 2006, Google Translate and Wikipedia were blocked.

Indeed, a unique feature of the GCC states' cyber landscape is the prevalence of religion in their CS strategies. In 2010, Saudi Arabia's Commission for the Promotion of Virtue and Prevention of Vice (the Haia) announced that it would establish a unit to fight cybercrimes. The Haia's initial focus was the online blackmail of women. A 2002 study conducted by Harvard Law School found that proxy serves in Saudi Arabia filtered and blocked sexually explicit content. In 2013, the Saudi Communications and Information Technology Commission (CITC) blocked about 400,000 pornographic sites. In August of 2014, the Haia asked the Ministry of Interior to arrest cyber-offenders who insult Allah, which is unspecific enough that the ministry can use this power almost indiscriminately.

Organizations in GCC countries have also taken measures to strengthen CS. Saudi governmental bodies like the Capital Markets Authority and the Riyadh city government have launched in-house or contracted efforts to protect data. Some organizations are building their own CS teams instead of outsourcing to third parties. Following the 2012 attacks, Aramco moved its outsourced IT services in-house. Likewise, the Saudi Electric Company (SEC) has placed special emphasis on CS for its electricity-generating systems. Not long ago, the SEC viewed the production side as a separate, closed system rather than as outward-facing. In revising this traditional view, the company was acknowledging that production is also exposed to cyber-threats.

Finally, GCC countries' CS measures have been considerably influenced by external actors. The United States is reportedly providing GCC states with cyber-attack defense assistance, especially those that provide intelligence about Iranian arms in return. So far, Saudi Arabia, the UAE, and

Bahrain are believed to have received such help. Bahrain also worked with the U.S. Department of Defense to develop civilian and military CS capabilities. Oman's Electronic Transactions Law and Qatar's Electronic Commerce and Transactions Law both draw on the UN Model Law on Electronic Commerce and the Model Law on Electronic Signatures.

Conclusion

GCC states are taking measures to strengthen CS, especially in free trade zones and key economic sectors. Capacity-building efforts, including CS skill development and enhancing educational awareness at various levels, need to be designed with the aim of enhancing cyber-defense capabilities.

In order to tackle internal CS threats, GCC states are taking measures to increase political authority and governing capacity. Cultural and sociopolitical factors also play key roles in GCC economies' cyber crime-fighting initiatives. In the absence of comprehensive laws, courts' judgments may be influenced by Sharia. Because they fall under individual judges' discretion, the punishment for data breach-related crimes are likely to be unpredictable and unclear. Ultimately, the lack of pan-GCC laws means that foreign businesses operating in the region may struggle with a number of compliance challenges.

Footnotes:

[1] Al-Saud, Naef Bin, A. 2012. "Cybersecurity Strategies." *JFQ: Joint Force Quarterly* 64(1): 75–81.

[2] Brenner, J. F. 2013. "Eyes wide shut: The growing threat of cyber attacks on industrial control systems." *Bulletin of the Atomic Scientists* 69(5): 15-20.