UAESF2016
UAE Security Forum

Bridging the Cybersecurity Talent Gap

Prepared by:
The Arab Gulf States Institute in Washington

Event Report

#1

2016

The Arab Gulf States Institute in Washington (AGSIW), established in 2014, is an independent, non-profit institution dedicated to increasing the understanding and appreciation of the social, economic, and political diversity of the Arab Gulf states. Through expert research, analysis, exchanges, and public discussion, the institute seeks to encourage thoughtful debate and inform decision makers shaping U.S. policy regarding this critical geo-strategic region.

Arab Gulf States Institute in Washington
1050 Connecticut Avenue, NW
Suite 1060
Washington, DC 20036

This publication can be downloaded at no cost at www.agsiw.org.

About the UAE Security Forum

Raytheon Company is the sponsor of the UAE Security Forum 2016.

With the increasing digitization of Gulf societies and the massive amounts of personal and sensitive information circling the globe every nanosecond, it is all too clear that strong cybersecurity is vital to keeping government, private sector, employer, and citizen information safe from malicious hacking, state-sponsored cyber espionage, or worse.

The need for cyber talent in the Gulf Cooperation Council states has never been more urgent, but the reality is that cyber talent is difficult to find, and even more difficult to attract.

To effectively build a cyber workforce of the future, new approaches and technologies are needed to streamline critical aspects of recruiting, hiring, workforce planning, and training.

To help bridge this talent gap, the Arab Gulf States Institute in Washington, in partnership with Raytheon and Khalifa University, is bringing government officials, educators, and employers together in Abu Dhabi to work to inspire the cybersecurity talent of tomorrow.

For more information visit www.uaesf.org.

February 11, 2016

Bridging the Cybersecurity Talent Gap

Introduction

The Middle East is fertile ground for cyber criminality due to its extensive use of technology and high value targets. In the Gulf Arab states, cyberattacks targeting key installations cost an estimated $1 billion annually and further losses are expected in part due to activities of hacker groups like the "Desert Falcons" targeting businesses.[1] Cyber criminals and hacktivists are chiefly motivated by an assortment of financial, social, and political objectives.[2] Yet, cyber capability is increasingly an integral part of economic development and many states have adopted it as a key part of their economic plans while attempting to balance against risk. The United Arab Emirates' ambitious digitalized national development agenda, which assures continued patterns of innovation, productivity, and economic growth, exists within a cyber threat environment.

As a society, the UAE is decidedly connected and this makes it easier to target. Connectivity induces vulnerability. The 2013 United Nations' Broadband Commission report stated that 85 percent of UAE residents are online, which in terms of Internet usage ranks it third in the Middle East and 17th globally compared to the United States in 24th place.[3] The UAE is also now the global leader in smart phone penetration,[4] but also ranked fifth globally among "most at risk."[5] In 2014, it saw a 400 percent rise in targeted attacks reaching nearly five percent of the global total, up from less than one percent in 2013,[6] while Dubai police received an incredible 1,549 reported cases of cyberattack.[7] Difficulties with detection and more sophisticated attack methods account for the sharp rise of incidents. Increases in the response times after an attack rose from an average of five days in 2013 to 59 days in 2014.[8] Despite the soaring 91 percent increase in the number of global targeted attacks, the UAE's Internet security profile improved in terms of the number of security threats across all categories from its 2012 world rank of 41 to 47 in 2014.[9] This reduction demonstrates that cyber defenses can work.

1 ICS Cyber Security Forum, "ICS Cyber Security Energy & Utilities Forum and Exhibition."
2 UAE National Electronic Security Authority, "The National Cyber Security Strategy," 6.
3 Sinclair, "UAE has third most internet users."
4 Fox, "The 15 Countries With the Highest Smartphone Penetration."
5 ***The National***, "UAE mobile users risk sharing."
6 John, "One-third of UAE firms."
7 ***The National***, "More than 1,500 cybercrime cases."
8 John, "One-third of UAE firms."
9 Malek, "UAE in cyber security talks."

The UAE Cyber Challenge

Information is a strategic commodity in today's globalized economy, within which cyberspace is a core dependency. The UAE has benefited from the digital economy and will pave the path toward realizing Vision 2030. The challenge is that the volume and speed of dangerous incursions to the accessibility, integrity, and resilience of the UAE's critical networked systems and infrastructures is both real and mounting. Threats stem from data infringements, criminal activity, and service disruptions.[10] The UAE's principle cybersecurity challenge is rooted in its broader national context as a country defined by the Internet of Things. Therefore, the necessity of and reliance on cyber capability underwrites the UAE's national security architecture. Cyber insecurity is a strategic threat.

Threats to the UAE's networked defense sector infrastructure are dangerous. They are also on the rise and driven by an interest in capabilities that governments are procuring.[11] The UAE military C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) systems are the first target in tactical cyberattacks aimed at intelligence gathering.[12] Its integrated missile defense platform necessitates more rigorous protection from cyber threats.[13] Plans in place for a network-based integration of the armed forces' core capabilities bring benefits and consequences in tandem. Capabilities grow, but cyber criminals have a new high value target.[14] To counteract vulnerability, the UAE aims to launch a military cyber command in the Armed Forces General Headquarters to run in parallel to the National Electronic Security Authority (NESA).[15] From a strategic standpoint, it is clear that cyber capability, cyber defense, cyber doctrine, and cyber diplomacy have growing implications for the UAE virtual threat environment.

Threats to the UAE's networked defense sector infrastructure are dangerous. They are also on the rise and driven by an interest in capabilities that governments are procuring.

The reliance on cyber capability in energy, finance, aviation, tourism, and governmental service sectors presents unique challenges. Cyber insecurity in these realms is a tax on the UAE's economic growth. Indeed, the same features of its economy that make it a success also expose risks. Government online portals are particularly vulnerable to cyberattacks because they are targeted.[16] Retired Major General Al Buainnain said, "…having the most advanced infrastructure makes you the most vulnerable."[17] To bolster cyber defense, the UAE is expected to double its cybersecurity budget to $10 billion within the next decade.[18] This increased budget is a needed investment given KPMG's survey, which indicated one-third of

10 Hathaway et al, "Cyber Readiness Index 2.0," 1.
11 Malek, "UAE is vulnerable to cyber attacks."
12 Mitreski, "The Case for a UAE Cyber Defence Doctrine."
13 Weisgerber and Mehta, "Fighters, Missiles and Transport."
14 ***Gulf News***. "Success of the UAE defence strategy."
15 Thomas, "UAE Military To Set Up Cyber Command."
16 Malek, "UAE is vulnerable to cyber attacks."
17 ***The Business Year***, "UAE Ministry of Economy," 97.
18 ICS Cyber Security Forum, "ICS Cyber Security Energy & Utilities Forum and Exhibition.

surveyed UAE firms reported cybersecurity breaches in 2015 and among them just 50 percent had cyberattack contingency measures in place. More worrying, only half of those hacked were aware of it.[19]

Perceptions about cybersecurity are another key challenge. Generally, UAE cyber practitioners downplay the role of internal cyber threats – the biggest source of insecurity. Aruba Networks revealed the UAE's GenMobile workforce, who integrate their mobile device into daily life, are "far more willing to share company data, and are notably oblivious towards security."[20] It reported that 62 percent habitually shared their work and personal devices, 14 percent did not have passwords, and 11 percent did not install any security measures so they could share more easily while 37 percent of UAE businesses did not have a basic mobile security policy in place.[21] Kaspersky placed the UAE 19th globally among countries facing the greatest risk of online infection in 2015 positioning it as a "high risk" country with 53 percent of infections coming from local threats.[22] GenMobile employees will continue to represent a key component of the UAE's national workforce and their risky behavior needs attention; the strategy will require a human-to-human approach rather than one that is device-focused. The associated challenge is to bridge the talent gap and create a future "cyber defense force."

Kaspersky placed the UAE 19th globally among countries facing the greatest risk of online infection in 2015 positioning it as a "high risk" country with 53 percent of infections coming from local threats.

The UAE needs more human capital for its cyber defense force, but it faces predicaments regarding recruitment, hiring, and training in cyber fields. In terms of barriers recruiting fresh talent, Raytheon and the National Cyber Security Alliance (NCSA) conducted a survey on cyber career interest and educational preparedness of millennials (ages 18 to 26) in 12 countries, including the UAE. Although there are differences between countries, there are also commonalities that lend themselves to policy design. Key findings include: evidence that schools are not providing cyber relevant activities and career information; the skills millennials want to develop are the same skills needed for a cyber career; millennials need more interaction with cyber professionals; mentoring programs have a positive impact; and females are less informed about careers in cybersecurity than males. Identifying these problems is an important step toward designing solutions to narrow the cyber talent gap.

UAE Cybersecurity Strategy

The UAE's national cybersecurity strategy context sits within the broader Gulf context, which has become a flashpoint for cyber conflict – cyberspace being an arena for clandestine struggle. A distinctive feature of the Gulf is the governments' extensive use of cyber techniques for covert engagement with other states, second only to the Korean peninsula.[23] Iranian cyberattack capabilities are of deep concern as Gulf Arab states have been attacked and imagine they will

19 John, "One-third of UAE firms."
20 ***The National***, "UAE mobile users risk sharing."
21 Ibid.
22 ***Albawaba Business***, "Kaspersky Lab reports UAE among the top-20 countries."
23 Lewis, "Cybersecurity and Stability in the Gulf," 1.
24 Ibid, 2.

be again. Also, concerns are rising about Israeli cyber capabilities.[24] Cyber activity in the Gulf is therefore reflective of the geopolitics of the region. The Gulf Cooperation Council strategy is to grow its cyber defensive capabilities and make efforts for the states to work together more successfully to discourage future threats. However, acknowledging the Gulf region's strategic and economic significance globally, a cyberattack that obstructs oil production could potentially intensify into armed conflict with serious repercussions for international security. Within the framing of this wider landscape, the UAE developed its national cyber strategy.

Cyber activity in the Gulf is therefore reflective of the geopolitics of the region.

The UAE government has committed to strengthening the effectiveness and resilience of its cybersecurity framework. The NESA, the UAE's federal body managing the country's overall cyberspace, published a national cyber strategy with accompanying policies and standards in June 2014.[25] The contents comprise the National Cyber Security Strategy (NCSS), Critical Information Infrastructure Policy (CIIP), and the UAE Information Assurance (IA) standard, which together form the heart of UAE national cybersecurity and ICT infrastructure approach. Compliance with the above is obligatory.[26] Additionally, there has been heavy investment in awareness campaigns to educate the public about new vulnerabilities, attacks, and incidents from hacktivists, organized criminals, and industrial spies. In a recent interview, Ilias Chantzos, Symantec's senior director of government relations and public affairs program in Europe, the Middle East, and Africa stated that "I've seen dramatic evolution in a positive way here…It's important to bear in mind that, in places like the UAE, the Government has been pioneering initiatives and we've seen a big take-up of technology."[27]

Aside from the considerable investment in crosscutting initiatives, the UAE has an observable emphasis on educational initiatives not only for mobile users, who are often easy targets for cyber criminals, but also children and the general public. Educational initiatives for child online safety programs are offered through the Ministry of Interior's Child Protection Centre.[28] The initiative informs children, young people, parents, teachers, and library staff about cyber safety issues and educates the public on online safety through information, resources, and practical advice.[29] Beyond this, hackathon competitions for university students are also increasingly common. Longer-term schemes in the cyber field include the opening of Khalifa University's Information Security Research Center (ISRC), which offers the country's only MSc and PhD in cybersecurity. The center focuses on innovative techniques, protocols, and systems for identifying cybersecurity threats, assessing risks, and protecting information and communication infrastructures while boosting capability in confidentiality, integrity, availability, authentication, accountability, and forensics.[30] ISRC's C3 cyber curriculum (cyber communication, culture, and certification) supports the development of local cyber expertise. The aim is to enable UAE nationals with enough cyber training to secure Critical National Infrastructures (CNI), Industrial Control Systems like supervisory control and data acquisition

25 McBride, "UAE cyber-security authority unveils policies, standards."
26 *The Business Year*, "UAE Ministry of Economy," 97.
27 Malek, "UAE in cyber security talks."
28 Jamaluddin, "Cyber safety for children stressed."
29 CYBER C3 Portal, "CYBER C3 Portal: Government Cyber Safety Initiatives."
30 Khalifa University, "Information Security Information Center (ISRC)."
31 CYBER C3 Portal, "CYBER C3 Portal: Government Cyber Safety Initiatives."

(SCADA), and the Critical Information Infrastructures (CII).[31]

Beyond an articulated cyber strategy and various cyber initiatives, legal measures are also in place and specific legislation exists on cyber crime such as Federal Law by Decree No. 5 of 2012 on Cyber Crimes, Federal Law No. 2 of 2006 on the Prevention of Information Technology Crimes, and Federal Law No. 1 of 2006 on Electronic Commerce and Transactions.[32] Technical cyber issues are addressed by aeCERT, an officially designated national body responsible for research and analysis projects for cybersecurity. It sets standards, best practices, and the guidelines to be applied in the private and public sector. There is also a Certified Professional Statistics Database that holds this record of public sector professionals certified under the aeCERT.[33] On an organizational level, the UAE has formally recognized the General Policy for the telecommunications sector and issued Cabinet Resolution No. 21 of 2013 regarding information security regulation in government entities and assigned the TRA as the agency responsible.[34] The UAE is working with these agencies on new data protection and smart grid initiatives as part of its national strategy, but despite these efforts the regulatory landscape has to be addressed in terms of implementing policies in the fullness they were intended. Chantzos said, "We're not there yet…It all boils down to how quickly the industry will adapt here."[35]

As mentioned, the UAE tops the list of communication system breaches across the Middle East. Fortunately, the UAE's need for cybersecurity is paired with the foresight and capacity to invest in a range of cutting-edge cyber defense capabilities. The UAE alone represents 41.5 percent of total Middle Eastern security software maintenance and license spending.[36] Beyond state-of-the-art technical cyber defense capabilities, the UAE's leadership understands that defending against attacks alone is an inadequate strategy. It is therefore shifting from a reactive to proactive operating mode. Current strategy aims to keep public and private organizations constantly informed of the ongoing, changing nature of the risks they face so they can better assess the type, timing, and occurrence of an attack. Information about and understanding of an attack is key to the next generation of information security in the UAE.[37] On the whole, the UAE's scorecard is a balance of some great initiatives and demonstrated results, but reveals there is plenty more to do to consolidate progress and achieve more.

Fortunately, the UAE's need for cybersecurity is paired with the foresight and capacity to invest in a range of cutting-edge cyber defense capabilities.

UAE Cybersecurity Gaps

The truth is that no country is cyber ready.[38] Cyber threats evolved so quickly that all governments around the world are scrambling to keep pace with the developments and institutionalize the correct frameworks and protocol. In the race to get measures rapidly in

32 ITU, "Cyber Wellness Profile: United Arab Emirates," 1.
33 Ibid, 2.
34 Ibid.
35 Malek, "UAE is vulnerable to cyber attacks."
36 Virginia Economic Development Partnership, "Cyber Security Export Market: United Arab Emirates," 6.
37 Gomes, Ian. "The cyber security threat from within."
38 Hathaway et al, "Cyber Readiness Index 2.0," 1.

place, the UAE is to be commended. But, there is a lot to be done as threats to the UAE are pervasive, risks are mounting, and cyber criminals are stealthier than ever. Broadly speaking, to stay ahead of increasingly numerous and sophisticated cyberattacks, all employees in all organizations must be made more aware of the new threat environment, enabled to cope with it, and identified if they do not follow protocol. Organizations, public and private, must address fundamental human practices, inculcated culture, and workplace behaviors that create cyber vulnerability. In practice, this means better integrating cybersecurity into general risk management approaches aimed at all staff as well as investing in continuing education for all senior management as well as board members.

Broadly speaking, to stay ahead of increasingly numerous and sophisticated cyberattacks, all employees in all organizations must be made more aware of the new threat environment, enabled to cope with it, and identified if they do not follow protocol.

There is no single solution and the approach to cybersecurity is evolving with the threat; however, a shift of focus from protection and compliance is critical.[39] Organizational managers need to adopt a truly collaborative approach to cybersecurity, which for instance means that information about close calls is distributed. Compartmentalization stifles proactive defense at times. Tim Allen, the general manager of QinetiQ in the UAE, said "I think [the government is] wrestling with the fact that historically some of these issues have been dealt with in isolation by government departments."[40] This challenge requires a modification to the UAE's engrained governance mentality and habituated organizational practice of operating in isolation and departmental opacity. More trust must be built to generate a greater willingness to share information and collaborate with other departments and agencies, which all too often are seen as competitors.

According to ITU, the U.N. specialized agency for information and communication technologies, the UAE has some gaps that impact its overall cyber wellness score. The ITU report, Cyber Wellness Profile: United Arab Emirates, highlighted the absence of a clear national governance roadmap for cybersecurity, the lack of national bench marks or referential to measure cybersecurity development, and no officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards. It also mentioned there is no framework for the certification and accreditation of national agencies. The ITU reported information was unavailable on an official inter-state framework for sharing cybersecurity assets across borders and no intra-state framework for sharing cybersecurity assets within the public sector in the UAE seemed to exist. There were also no officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.[41] This does not mean that these frameworks and programs do not exist – in whole or part – but it notes they have not been publicized, if they are in place or being developed. These gaps must be contextualized against the scorecard of states worldwide, which on the whole looks relatively similar to the UAE at this time.

39 Gomes, "The cyber security threat from within."
40 Malek, "UAE in cyber security talks."
41 ITU, "Cyber Wellness Profile: United Arab Emirates."

Conclusion

The UAE's general cyber threat landscape has evolved past the vandalism of lone hackers toward sophisticated, assiduous threat tools employed by "cyber brigades" to steal, undermine, or entirely disrupt the security of the state by capturing the increasing quantity and value of data being generated. The sophistication of cyberattacks is putting organizations at risk. But, within the balance of threat and opportunity, the UAE has tied its future success to technology, which fortifies governmental commitment to securing its strategic infrastructure to preserve national security and social stability. It has committed significant resources to foster improved cyber defenses and develop more technical cyber capability among its people. It has also completed the initial – and most vital – part of obtaining cyber readiness, which is to articulate and disseminate a National Cyber Security Strategy aligning the country's economic vision with national security imperatives. At this time, the path to advancing the UAE's cyber strategy is to transcend the priority areas and aspirational objectives set out and move toward actualizing the articulated goals by operationalizing more concrete measures. Strategic cyber efforts, aimed at capturing the technological confluence between economy and (in)security, will produce a reliable picture from which the UAE government can assess its cybersecurity maturity. This snapshot of current cyber wellness will help create a framework to develop new policy, strategy, and operational and institutional initiatives; identify specific resourcing needs; construct revisions to regulatory and legislative instruments; and manage levers of the marketplace most efficiently.

No country is cyber prepared. For now, collaboration will remain crucial for the UAE in terms of benefiting from cyber lessons learned, identifying effective policies, and gaining access to cutting-edge technical advice offered by its allies. The United States is willing to share its technology with the UAE[42] and partnerships like this and others will boost its cyber defense while simultaneously strengthening its position as a valuable partner to its allies.[43] The UAE has been working with NATO countries on cyber topics and this is an ideal application of the Istanbul Cooperation Initiative. Ultimately, cyber diplomacy offers many opportunities as it aims to identify mutually satisfactory solutions to shared challenges felt worldwide. Cybersecurity subjects touch the spectrum of diplomatic activity related to trade, foreign, defense, and economic affairs. Critical capability now lies in a country's ability to access cyber capital by effectively engaging diplomatically on cyber topics. Allocating funding for international dialogue meetings and training on cyber issues is a worthy investment while simultaneously investing in national talent development and growing the UAE's domestic cyber industry (hardware, software, and training). Active collaboration between business, government, and education systems, as well as a well-trained and aware citizenry are also key. There is no single bulletproof cyber defense mechanism and the best cyber defense is a diversified one.

42 Virginia Economic Development Partnership, "Cyber Security Export Market: United Arab Emirates."
43 Mitreski, "The Case for a UAE Cyber Defence Doctrine."

Works Cited

Albawaba Business. "Kaspersky Lab reports UAE among the top-20 countries facing the greatest risk of online infection in 2015." December 16, 2015. http://www.albawaba.com/business/pr/kaspersky-lab-reports-uae-among-top-20-countries-facing-greatest-risk-online-infection-2.

The Business Year. "UAE Ministry of Economy" (2015): 95-97. https://www.thebusinessyear.com/Content/Publication/01e78f07-5b0b-4183-b1c3-0163382d9c69.pdf.

CYBER C3 Portal. "CYBER C3 Portal: Government Cyber Safety Initiatives." Accessed January 5, 2016. http://uaecyber.com/en/about/government-initiatives/government-cyber-safety-initiatives/.

Fox, Zoe. "The 15 Countries With the Highest Smartphone Penetration." *Mashable*. August 27, 2013. http://mashable.com/2013/08/27/global-smartphone-penetration/#EQ4BhYFjQ5qX.

George, Joseph. "Mideast firms don't care about cyber threat." *Emirates 24/7*. March 4, 2015. http://www.emirates247.com/business/technology/mideast-firms-don-t-care-about-cyber-threat-2015-03-04-1.583122.

Gomes, Ian. "The cyber security threat from within." *The National*. March 5, 2015. http://www.thenational.ae/business/technology/the-cyber-security-threat-from-within.

Gulf News. "Success of the UAE defence strategy." December 14, 2014. http://gulfnews.com/news/uae/government/success-of-the-uae-defense-strategy-1.1426762.

Hathaway, Melissa, Chris Demchak, Jason Kerben, Jennifer McArdle, and Francesca Spidalieri. "Cyber Readiness Index 2.0 A Plan for Cyber Readiness: A Baseline and an Index." *Potomac Institute for Policy Studies* (November 2015): 1–48. Accessed January 10, 2015. http://www.potomacinstitute.org/images/CRIndex2.0.pdf.

ICS Cyber Security Energy Forum 2015. "ICS Cyber Security Energy & Utilities Forum and Exhibition." Accessed January 3, 2016. http://www.csuae.org/index.html.

Injazat Data Systems. "Cloud Services in the UAE poised for 40+ per cent growth rate through 2016." Accessed January 5, 2016. http://www.injazat.com/Lists/News/DispForm.aspx?ID=117&Source=http%3A%2F%2Fwww%2Einjazat%2Ecom%2FLists%2FNews%2FAllItems%5FPages%2Easpx.

ITU. "Cyber Wellness Profile: United Arab Emirates." Last modified February 19, 2015. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/United_Arab_Emirates.pdf.

Jamaluddin, Shamila. "Cyber safety for children stressed at Ministry's summit." *The Gulf Today*. November 17, 2015. http://gulftoday.ae/portal/5e5e0843-c774-4a23-9d16-6b89b18a2468.aspx.

John, Issac. "One-third of UAE firms in cyber security breaches." *Khaleej Times*. December 21, 2015. http://www.khaleejtimes.com/business/local/one-third-of-uae-firms-in-cyber-security-breaches-.

Khalifa University. "Information Security Information Center (ISRC)." Accessed January 5, 2016. http://www.kustar.ac.ae/pages/information-security-research-center-isrc/12197.

Lewis, James Andrew. "Cybersecurity and Stability in the Gulf." *Center for Strategic & International Studies*. January 6, 2014. http://csis.org/publication/cybersecurity-and-stability-gulf.

Malek, Caline. "UAE in cyber security talks to combat latest threats." *The National*. September 4, 2014. http://www.thenational.ae/uae/technology/uae-in-cyber-security-talks-to-combat-latest-threats.

Malek, Caline. "UAE is vulnerable to cyber attacks." *The National*. August 24, 2014. http://www.thenational.ae/uae/technology/uae-is-vulnerable-to-cyber-.

McBride, Stephen. "UAE cyber-security authority unveils policies, standards." *ITP.net*. June 25, 2014. http://www.itp.net/598777-uae-cyber-security-authority-unveils-policies-standards.

Mitreski, Aleksandar. "The Case for a UAE Cyber Defence Doctrine." *Institute for Near East and Gulf Military Analysis*. October 7, 2013.

The National. "More than 1,500 cybercrime cases reported to Dubai Police." February 8, 2015. http://www.thenational.ae/uae/government/more-than-1500-cybercrime-cases-reported-to-dubai-police.

The National. "UAE mobile users risk sharing their employer's data, report says." April 17, 2015. http://www.thenational.ae/uae/technology/20150417/uae-mobile-users-risk-sharing-their-employers-data-report-says.

PricewaterhouseCoopers (PwC). "PwC's Global Economic Crime Survey shows fraud reported by 21% of organisations in the Middle East compared to 37% globally." February 26, 2014. http://www.pwc.com/m1/en/media-centre/2014/global_economic_crime_survey_shows_fraud_reported.html.

Raytheon. "Securing Our Future: Closing the Cybersecurity Talent Gap." October 2015.

Sinclair, Kyle. "UAE has third most internet users in the Middle East." *The National*. October 3, 2013. http://www.thenational.ae/business/technology/20131003/uae-has-third-most-internet-users-in-the-middle-east.

Thomas, Bindiya. "UAE Military To Set Up Cyber Command." *Defenseworld.net*. September 30, 2014. http://www.defenseworld.net/news/11185/UAE_Military_To_Set_Up_Cyber_Command#.VokO8vl96Uk.

UAE National Electronic Security Authority. "The National Cyber Security Strategy." 2015.

Virginia Economic Development Partnership. "Cyber Security Export Market: United Arab Emirates." *George Mason University (School of Public Policy): Virginia Economic Development Partnerships (VEDP) Going Global Defense Initiative* (2014).

Weisgerber, Marcus and Aaron Mehta. "Fighters, Missiles and Transport: GCC Spending Priorities Take Shape." *Defense News*. November 16, 2013. http://www.defensenews.com/article/20131116/DEFREG04/311160013/.

The World Bank. "Information & Communication Technologies Overview." Accessed January 10, 2016. http://worldbank.org/en/topic/ict/overview.