Virginia ExportVirginia.org
BUSINESS WITHOUT BORDERS

Cyber Security Export Market: Saudi Arabia

2014

Sponsored by the Virginia Economic Development Partnership's (VEDP)
Going Global Defense Initiative

George Mason University (School of Public Policy)

This study was prepared under contract with the Commonwealth of Virginia, with financial support from the Office of Economic Adjustment, Department of Defense. The content reflects the views of the Commonwealth of Virginia and does not necessarily reflect the views of the Office of Economic Adjustment.

Virginia loves Exports

Virginia
ExportVirginia.org
BUSINESS WITHOUT BORDERS

CONTENTS

Virginia ExportVirginia.org BUSINESS WITHOUT BORDERS

CONTENTS

EXECUTIVE SUMMARY

- Saudi Arabia offers a prime market for cyber security exports. Saudi Arabia's ample defense spending, which exceeded $56 billion in 2012 and partnership with the United States (US) provides considerable opportunities for US defense firms.

- The market for cyber security exports is expected to burgeon in upcoming years, increasing by 30 percent to $37.5 billion by 2016. Related areas of investment such as Information Technology (IT) and software have also grown. For example, software spending has increased more than 10 percent year-over-year.

- Saudi Arabia has demonstrated sustained political and economic stability for several decades. The business climate is relatively favorable; however, the kingdom does possess some unique cultural characteristics. Foreign firms must be prepared to navigate gender inequality, censorship and the influence of *Shari'ah* law.

- In light of recent cyber-attacks, Saudi Arabia has established regulatory and legislative frameworks to support cyber safety. The kingdom is also developing a National Information Security Strategy. Correspondingly, Saudi Arabia has increased cyber security spending and investment across government agencies and local governments.

- The US has been a key player in shaping Saudi Arabia's cyber defenses. The US has coordinated cyber security policies with Saudi Arabia and organized trade missions to introduce US defense firms to the government officials.

- Given the collaborative relationship between the US and Saudi Arabia in addition to the kingdom's own efforts there is a strong need for surveillance technology, advanced communication systems, detection equipment, cyber-attack alarms, cyber intrusion prevention technology. Nearly every level of government, from local to national, covering a wide range of issues, from finance to science technology, have devoted increased resources to build up cyber security defense going forward.

- In addition to public demand, there is a role for private cyber security exports in the energy, financial services, information technology (IT), and communications industries.

CYBER SECURITY MARKET

GOVERNMENT PROGRAMS & POLICIES

In light of the growing threat of cyber-attacks, Saudi Arabia has stated that it will begin to concentrate on online data, information, and infrastructure protection with increased investment in cyber defense measures.[1] Agencies from varying levels of the government have implemented new initiatives to bolster cyber defense. From the Capital Markets Authorities to city governments, agencies have implemented internal strategies and solicited private help.[2] These new policy initiatives have translated into increased spending. For instance, the Saudi Arabian Monetary Agency spent more than $20 million on cyber security in 2013, and the Ministry of Petroleum and Mineral Affairs spent $8.7 million.[3]

In 2011, the Ministry of Communications and Information and Technology published its proposed National Information Security Strategy to apply to all levels of the government and unify individual efforts.[4] The proposed objectives of the National Information Security Strategy are illustrated in **Figure A.**

Figure A: Objectives of the National Information Security Strategy

Source: Kingdom of Saudi Arabia. Ministry of Communications and Information and Technology.

[1] (International Trade Administration, 2013).
[2] (Knickmeyer, 2013).
[3] (Naseba, 2013
[4] (KSA, NISS, 2012).

In addition to the National Information Security Strategy, the Ministry of Communications and Information and Technology have made several recommendations for future development of information technology (IT) security infrastructure. The ministry proposed a centralized enforcement regime with a designated group of "forensic specialists" to monitor media communications.[5] National and international coordination was also encouraged.[6] These areas will likely guide future investment and procurement.

It appears that Saudi Arabia is also interested in reducing unemployment through its investment in cyber security; therefore, the export of products and services that can be utilized and implemented by Saudi Arabian users will be more attractive to the government. Specifically Saudi Arabia hopes to expand jobs for females and unemployed males with limited formal education but sophisticated technology skills.[7]

CYBER ATTACKS

Not only is the government poised to increase investment in cyber defense, but also recent cyber-attacks have elevated demand and awareness to an even higher level. Saudi Arabia is a major target for cyberattacks and other forms of cyber harassment and violation. Saudi Arabia is the number two global target for online spam.[8] In 2013 alone, there have been a variety of attacks on Saudi Arabia. The national police's website was corrupted to showcase the propaganda of Shiite Muslims.[9] In August 2013, the search results for Google searches for "Saudi King Abdullah" were hacked to respond with a message reading, "Hey King of SAUDI ARABIA. Please Don't Support to Terrorist Military of Egypt" (sic).[10]

The cyberattack against Aramco, one of Saudi Arabia's state-run oil companies, was the most egregious cyberattack in the kingdom to date.[11] Aramco is the largest exporter of oil and natural gas in the world and the sixth largest oil refiner.[12] The attack, which occurred in 2012, shut down the company's computer systems for 10 days.[13] Investigations point to differing sponsors of the attack. Some accounts suggest that the attack was initiated from within the kingdom from Shia groups, others suggest that the attack was perpetrated outside of the kingdom's borders from other states in the region.

The most recent cyberattack occurred in September of 2013.[14] The Ministry of the Interior warned of attacks on Saudi Arabian cabinet ministries' websites and online infrastructure.[15] The Foreign Ministry, Ministry of Finance, Ministry of the Interior and Ministry of Labor were already attacked earlier in the year.[16]

In cases similar to these, where phishing and pharming scams are used, companies must rely on the judgment of employees to protect data and privacy. Consultative services and staff training appear to be areas of need that US defense firms could serve. Moreover, the increasing frequency and severity of these kinds of attacks on public and private entities provide US defense firms with an opportunity to export attack monitoring software as well as stress tests and other cyber security products.

---

[5] (KSA, NISS, 2012).
[6] *Ibid.*
[7] *Ibid.*
[8] (Knickmeyer, 2013).
[9] *Ibid.*
[10] *Ibid.*
[11] (EIU, Investigation Blames non-Saudis for Aramco Cyber-attack, 2012).
[12] (Saudi Aramco, 2013).
[13] (EIU, Investigation Blames non-Saudis for Aramco Cyber-attack, 2012).
[14] (EIU, Risk Briefing, 2013).
[15] *Ibid.*
[16] *Ibid.*

MARKET SECTORS & OPPORTUNITIES

According to the International Trade Administration (ITA), Saudi Arabia has an immediate need for surveillance technology, advanced communication systems, electronic detection equipment, cyberattack alarms, cyber intrusion prevention technology, and biometrics, as identified in **Figure B.**[17] Infrastructure-related investment, also incorporates a need for services and products that may be provided by US defense firms. Saudi Arabia expends considerable resources in this area; for example, in 2012, the government spent $9.4 billion on transportation infrastructure alone.[18] Saudi Arabia's state-owned firms also offer export opportunities. For example, after the 2012 cyberattack, Aramco announced $30 million in additional spending on cyber defense.[19] The Aramco incident also prompted other private sector companies to revisit cyber security, including IBM, Mobily and Symantec.[20]

Figure B: Areas of Opportunity for Cyber Security Exports

Areas of Cyber Security Export Opportunity ITA
Surveillance Technology
Advanced Communications Systems
Electronic Detection Equipment
Cyber Attack Detection Systems
Cyber Attack Prevention Technology
Bio Metrics

Source: International Trade Administration

US COLLABORATION

The US maintains an agreement related to critical infrastructure protection, providing an additional avenue of opportunity for US defense firms. The Technical Cooperation Agreement between the US and Saudi Arabia's Ministry of the Interior provides for the exchange of "advice, training, equipment and other resources" for security and critical infrastructure protection.[21] Civil defense and public security fall within the authority of the agreement, which can include cyber security.[22] Under the arrangement, the US has agreed to furnish resources and support procurement of private US defense firms on behalf of Saudi Arabia.[23]

Saudi Arabia's software market already commands a considerable amount of exports and investments. Together with the United Arab Emirates (UAE), Saudi Arabia accounts for 75 percent of spending on software in the Middle East.[24] The most recent trade data from 2010 shows that software spending rose 12.9 percent in one year.[25] Nearly half of the software spending was related to security and infrastructure

[17] (International Trade Administration, 2013).
[18] *Ibid.*
[19] (EIU, Software, 2013).
[20] (Knickmeyer, 2013).
[21] (Department of State, 2008).
[22] *Ibid.*
[23] *Ibid.*
[24] (EIU, Software, 2013).
[25] *Ibid.*

reinforcement.[26] Saudi Arabia's 2012 – 2016 Second National Action Plan outlines expectations for continued government investment in IT infrastructure.[27] In contrast to Saudi Arabia's desire to use the increased funding to create domestic jobs, there are concerns that government officials lack the necessary skills.[28] This gap suggests that there may be a future demand for IT training programs and/or contract workers.

MARKET TRENDS

The cyber security market in Saudi Arabia is currently centered around the protection of energy systems and the e-commerce space. The Saudi Arabian government and private sector have recognized that the energy infrastructure is vulnerable to cyberattacks.[29] Data management and cyberattack detection and prevention services would address the concerns of the energy sector. Foreign firms could also tap into government projects or the larger cyber security market by entering the e-commerce space, which is receiving considerable attention. Currently, Saudi Arabia is working to monitor bloggers, support online bill payment systems, oversee the expansion of Internet access, and monitor the burgeoning telecommunications industry.[30] The kingdom has also deployed an e-government campaign to streamline and construct electronic databases.[31] Foreign firms could access the market by working with the Saudi Electronic Data Interchange, which manages government transactions, the eGovernment Service Bus Program, which is centralizing online government databases, and/or Tabadul, the Saudi Arabian Electronic Exchange Company, which manages public investment in IT.[32] These trends offer opportunities to enter the cyber security market.

There are also trends underway in the technological environment in Saudi Arabia. The technological environment is rather advanced, but is still limited compared to the world's most developed countries. To illustrate, 54 percent of the population has access to the Internet today.[33] Household technological access has expanded dramatically in recent years. From 2008 to 2012, Internet usage increased by 50 percent.[34] By 2015, access is expected to enlarge to 72.5 percent of the population.[35] The recent build-up in online activities and coverage naturally corresponds to increased vulnerability to cyber threats. Notwithstanding the expanded access, all users are constrained by some degree of social censorship and government surveillance.

MARKET COMPETITION

There are several foreign firms already engaged in Saudi Arabia's cyber security market. Current players range from electronic manufacturing providers to technology firms and private defense firms. **Figure C** lists current market participants and the nature of the engagement in the kingdom's market.

---

[26] *Ibid.*
[27] *Ibid.*
[28] *Ibid.*
[29] (Roberts, 2012).
[30] (EIU, Overview of e-commerce, 2013).
[31] *Ibid.*
[32] *Ibid.*
[33] (World Bank, Internet Users, 2012).
[34] *Ibid.*
[35] (EIU, Data Tool, 2013).

Figure C: Current Market Participants

Company	Market Engagement
AirPatrol Corporation	Device identification and tracking
DataLocker	Encryption services and digital storage
Emagine IT	Leadership consulting related to IT and cyber security
FireEye	Cyber-attack prevention software
Glimmerglass Optical Cyber Solutions	Collection of electronic intelligence
Implant Sciences Corporation	Military technology products and services
Lockheed Martin	Intelligence-Drive Defense Framework
Microsoft	Manages online government bill-pay and transaction systems
OSI	Digital network management
Raytheon	Military technology products and services
SEL	Utility and infrastructure safety solutions
Sourcefire	Develops safe IT platforms
Tecore Networks	IT infrastructure provider
Symantec	Assesses cyber threats and attacks
IBM	Consumer IT security goods and services; digital infrastructure development

Source: United States. Department of Commerce. "Trade Mission to Saudi Arabia and Kuwait." U.S. Commercial Service. Sept 2013. Print.
http://export.gov/kuwait/build/groups/public/@eg_kw/documents/webcontent/eg_kw_065244.pdf.

For more information on Saudi Arabia's cyber security strategy and its partnership with the US, please refer to the following resources:

- Saudi Arabia's Draft National Information Security Strategy
- Technical Cooperation Agreement between the US and Saudi Arabia
- ITA trade mission to Saudi Arabia

MARKET ACCESS

IMPORT PARAMETERS

The import burdens and costs in Saudi Arabia are comparatively modest, but not minimal. This is particularly relevant to US defense firms seeking to export goods and services to the private sector in Saudi Arabia. Saudi Arabia's general importing parameters are illustrated in **Figure D.** At a minimum, it takes 17 days to complete the documentation preparation, receive customs clearance and technical controls, process ports and terminal handling and inland transportation, costing $1,054 USD with a simple average applied most favored nation (MFN) tariff of 4.9 percent.[36] Saudi Arabia is also a member of the

[36] (World Bank, Ease of Doing Business, 2013).

Gulf Cooperation Council (GCC), and therefore applies the GCC external tariff of five percent on nearly all products.[37] Saudi Arabia applies a heightened 12 percent tariff on certain products that compete with local producers, practically none of which apply to the cyber security market.[38] As a member of the WTO, Saudi Arabia binds its tariffs on the majority of US exports with an average tariff rate of 3.2 percent.[39]

Figure D: General Importing Parameters

General Importing Parameters	
Minimum Days for Document Preparation	17 days
Minimum Cost	$1,054 USD
Average MFN Tariff	4.9 percent

Source: The World Bank

Under the GCC, members receive preferential treatment compared to non-members, with a 10 percent price advantage for GCC originating products.[40] In addition to GCC advantages, domestic firms often receive preferential treatment.[41] Under the Government Tender and Procurement Law, government procurement is easier and more streamlined for domestic firms, whereas procedures are lengthier and stricter for foreign firms.[42] Saudi Arabia also prohibits the import of many categories of products. While these prohibitions do not generally apply to the cyber security market, they do fall outside of normal prohibitions given the religious and social restrictions in the kingdom.[43]

TRADE AGREEMENTS

Saudi Arabia maintains several trade agreements, which will support easier exporting arrangements for US defense firms and may also facilitate entrance into new markets. Currently, the US maintains a Trade and Investment Framework Agreement (TIFA) with Saudi Arabia.[44] The TIFA provides for the expansion of trading of goods and services between the US and the establishment of a Joint Commission on Economic Cooperation to promote increased trade and investment.[45] The TIFA also outlines opportunities for future trade in the area of intellectual property.[46] Saudi Arabia is also party to the US Middle East Free Trade Area Initiative (MEFTA).[47] The initiative, originally proposed in 2003, outlined a gradual plan to establish free trade with several Middle Eastern countries, including Saudi Arabia.

PROCUREMENT

As mentioned earlier, Saudi Arabia is also a member of the WTO and party to the plurilateral Agreement on Government Procurement (GPA).[48] Saudi Arabia signed onto the agreement in 2007. The GPA governs government procurement practices and supports transparency and fair treatment in such practices.[49] Notably, however, Saudi Arabia's military procurement terms appear to be determined on a

[37] (Department of State, 2011).
[38] *Ibid.*
[39] *Ibid.*
[40] (FedEx, 2013).
[41] (Latham & Watkins, 2010).
[42] (Latham & Watkins, 2010).
[43] (FedEx, 2013).
[44] (Trade Representative, Saudi Arabia - TIFA).
[45] *Ibid.*
[46] *Ibid.*
[47] (Trade Representative, MEFTA).
[48] (WTO, GPA, 2007).
[49] *Ibid.*

case-by-case basis.[50] The Saudi Government Procurement and Competition System governs much of the kingdom's procurement.[51] The system stipulates a bidding process for companies and provides uniform bidding procedures and time frames.[52] The procuring agency, however, maintains a high degree of discretion in determining the terms of acquisition.[53] The kingdom typically employs public tendering for procurement, but may also use special tendering or direct contracting in certain cases.[54] The government does not use a central tenders system for procurement. Each agency can conduct its own contracts. US exporters should communicate with individual agencies in order to pre-qualify and bid on contracts. Unlike in some other GCC countries, a Saudi agent is not required by the law for most government contracts. There might be other clauses such as training programs in the contract.

For additional information on Saudi Arabia's trade agreements, participation in the WTO, and procurement, please refer to the following resources:

- TIFA Agreement between the US Government and the Kingdom of Saudi Arabia
- Saudi Arabia's government website on trade agreements
- WTO's member profile on Saudi Arabia
- USTR analysis of trade barriers in Saudi Arabia
- Saudi Arabian General Investment Authority

Royal Decree M/58, "Government Tenders and Procurement," and Minister of Finance Decision 362, "Implementation of Government Tender and Procurement Law," are the primary regulations governing procurement processes.[55] Royal Decree M/58 outlines the public bidding process and gives priority to domestic firms.[56] Decision 362 stipulates that tenders be published in "*the Official Gazette* and two local newspapers at least once, through electronic means, on the website of *Umm Al-Qura Gazette* and the website of the advertising authority."[57] Tenders must be posted for a minimum of 30 days.[58] Very small government projects are not required to be publically published.[59] Certain military and electrical equipment are excluded from the requirement for public bidding as well.[60] Both individual and collective firms can bid on public tenders.[61] Most government contracts are subject to a five-year limit.[62] Such contracts are generally required to be submitted in Arabic, with some concessions for English speaking firms.[63] Notably, under *Shari'ah* Law, all firms contracting with the Saudi Arabian government are strictly liable for any and all losses.[64] Other than this stipulation and language requirements, the procurement process is relatively straightforward for foreign firms.

Published tenders may be difficult to find publically in English. However, there are a number of online services that provide access to databases of Request for Proposals (RFPs) and other Saudi Arabian

---

[50] (Trade Representative, Saudi Arabia, Foreign Trade Barriers, 2012).
[51] (Saudi's e-Government Program, 2013).
[52] *Ibid.*
[53] (Saudi's e-Government Program, 2013).
[54] *Ibid.*
[55] (Saudi Arabia, Government Tenders and Procurement, 2006).
[56] *Ibid.*
[57] (Saudi Arabia, Implementation of Government Tender and Procurement Law, 2007).
[58] Ibid.
[59] (Crowell Moring, 2013).
[60] Ibid.
[61] Ibid.
[62] Ibid.
[63] Ibid.
[64] (Crowell Moring, 2013).

tenders for a fee. Key contacts for procurement information and publication with the primary candidates for cyber security exports are listed in **Appendix I.** For the most extensive compilation of tenders available in English, please refer to **Appendix II**, which lists the current tenders related to cyber security from *Global Tenders.*

For additional information on open Saudi Arabian tenders, please refer to the following resources. Note, however, that certain government cites are in the process of being updated and/or not available in English:

- Saudi Tenders
- Global Tenders
- Information Technology Tenders
- Kingdom of Saudi Arabia Tenders
- Ministry of Finance Tenders List
- Ministry of Defense
- Umm Al-Qura Gazette
- Communication and Information Technology Commission Public Consultation Solicitation Page

MARKET SIZE & GROWTH

DEFENSE SPENDING & INVESTMENT

Defense spending comprises a considerable portion of the Saudi Arabia's GDP, and is clearly a main focus of government expenditure and development. In 2012, Saudi Arabia's total military expenditures reached approximately $56.3 billion.[65] In the same year, the defense industry accounted for 8.9 percent of GDP.[66] Similar to the performance of the larger economy, defense spending is closely tied to oil exports. Increases in oil prices allow the economy to grow and rising oil revenues pad the domestic budget.[67] More than a quarter of the budget, 26 percent, is furnished by oil revenues.[68] Revenues from oil exports allow the government to increase defense spending and have historically corresponded with military buildup.[69] Accordingly, there is a strong potential for increased security imports.

To date, Saudi Arabia has limited its investment in technology.[70] Technology serves as the primary venue from which a government can combat cyber security, therefore, it is expected that eventual investment in this area will be necessary. Accordingly, the cyber security market in Saudi Arabia is expected to burgeon, even in the next three years, growing by 30 percent to $37.5 billion in 2016. Cyber security spending has already reached considerably high levels, suggesting that the market is already primed for foreign imports. In 2013, public and private spending on cyber security in Saudi Arabia exceeded $6 billion.[71]

---

[65] (SIPRI, 2013).
[66] *Ibid.*
[67] (Chun, 2010).
[68] (Chun, 2010).
[69] *Ibid.*
[70] *Ibid.*
[71] (KSA, NISS Public Comment Document, 2012).

US AGENDA FOR SAUDI ARABIA

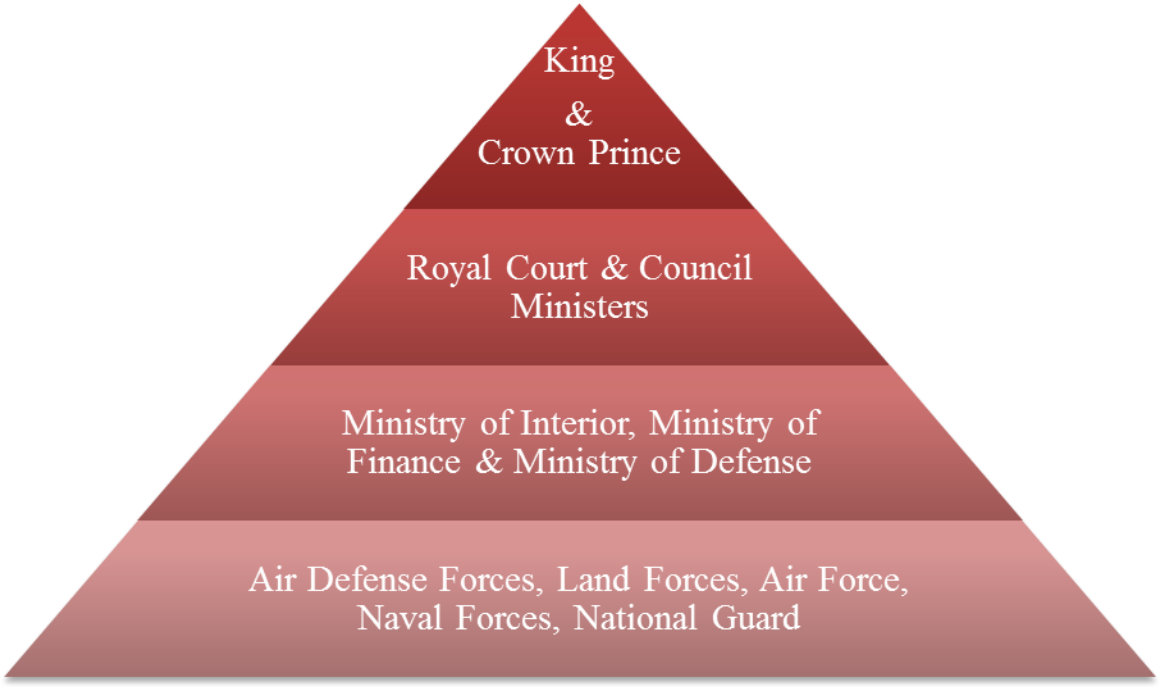
The US has mobilized Saudi Arabia's cyber security strategy, in part because of the long-standing relationship with the kingdom as well as the strategic value of its oil reserves and exports. Correspondingly, the Saudi Arabian cyber security strategy is shaped by and overlaps with the US's global cyber security agenda. The US has promoted cyber security policy models and encouraged international norms for cyberspace conduct.[72] The US has also promoted sovereign responsibility doctrines to encourage governments to monitor domestically originating cyberattacks.[73] As part of the US's cyber security agenda, the US Trade Administration organized trade missions to Saudi Arabia to couple the Saudi Arabian government's needs with private US security providers. The most recent mission was conducted by the Department of Commerce in September of 2013.[74] Recently, in the summer of 2013, the US began its direct support of Saudi Arabia's cyber defense systems in response to growing threats from Iranian attacks.[75] US agencies and existing policies have laid the foundation for successful engagements between US defense firms and the kingdom's government.

DEFENSE COMMAND STRUCTURE

The King and Crown Prince oversee the Royal Court and Council of Ministers, which govern the defense-related ministries and represent the top tier of the military command structure in Saudi Arabia. US defense firms would generally engage the Ministers of Defense, Interior and Finance as well as the Saudi Arabian intelligence agency in procurement contracts. The Minister of Defense oversees all of the branches of the military.[76] Saudi Arabia's military is divided into six branches: Land Forces; Naval Forces; Air Force; Air Defense Forces; Strategic Rocket Forces; and National Guard. The Ministry of the Interior and the Ministry of Finance are independent of the military branches.[77] The General Intelligence Presidency (GIP) is the primary intelligence agency.[78] The head of the GIP reports to King Abdul Aziz.[79] The agency is well funded with an estimated annual budget of $500 million.[80] The chain of command for the entire military structure is shown in **Figure E.**

[72] (GAO, 2010).
[73] *Ibid.*
[74] (International Trade Administration, 2013).
[75] (Shanker, 2013).
[76] (Saudi Arabia, Ministry of Foreign Affairs, 2012).
[77] (Woodson, 1998).
[78] (Cordesman, Obaid, 2004).
[79] *Ibid.*
[80] *Ibid.*

Figure E: Military Chain of Command



Source: US Central Intelligence Agency

MARKET ENTRY STRATEGY

AGENTS

Since 2001, foreign firms have not been required to employ a commercial service agent to contract with the government.[81] There are few government contracts which might be exceptions and need minority Saudi Arabian interest. Nevertheless, due to the cultural and institutional differences between the two countries, it is advisable to hire an agent who is knowledgeable about the procurement process and preferably, has access to the concerned Ministry. Agents can earn up to 10 percent in commission fees. Agency contracts should be carefully negotiated because termination is often tedious and difficult. Legal counsel must be sought. Saudi Arabian culture is relationship-based and values face-to-face interaction and trust building.

LOCAL PRESENCE

There are two primary business structures in Saudi Arabia, including limited liability corporations (LLCs) and joint stock companies.[82] Foreign firms are not required to partner with citizens or domestic businesses. LLCs are the most common business formations and can be wholly owned by foreign entities.[83] Joint stock companies can also be wholly foreign owned.[84]

---

[81] (Commercial Guide, 2011).
[82] (Saudi Arabia General Investment Authority).
[83] (Saudi Arabia General Investment Authority, 2013).
[84] *Ibid.*

For foreign firms desiring to establish a larger and more permanent presence in the kingdom, an LLC arrangement allows for greater flexibility in public and private business engagement and business promotion.[85] Foreign LLCs will, however, be subject to capitalization requirements and considerable oversight from the Saudi Arabian General Investment Authority (SAGIA).[86] Foreign firms can also establish multiple branches in the kingdom.[87] Firms desiring a more flexible business arrangement can pursue a temporary commercial registration, which is available to firms with a government contract.[88]
To register a business, foreign firms must work through the SAGIA and complete an Investment Licenses application, as well as file for an Investor Visa and Commercial Registration.[89] Foreign firms must also register with the Chamber of Commerce, Department of Zakat and Income Tax, General Organization of Social Insurance, Labor Office and the local municipality.[90]

LEGAL ISSUES

Saudi Arabia has recently reinforced its regulatory and legislative frameworks to support cyber safety.[91] Since 2002, the kingdom has enacted four landmark intellectual property (IP) laws, including, the 2002 Law of Trademarks, the 2003 Copyright Law, the 2004 Law of Patents, Layout-Designs of Integrated Circuits, Plant Varieties, and Industrial Designs and the 2010 Law of Trade Names.[92] This new legislation adds to the existing framework of 17 IP-related laws.[93]

In 2007, Saudi Arabia passed a major law to combat cybercrime.[94] The law set out to increase information security, protect digital rights for computer networks, enforce public interests and protect national economic interests.[95] Privacy rights are also enforced by Saudi Arabia's laws according to the kingdom's Basic Law of Governance, which prohibits the disclosure of private information and confidential communications.[96] Islamic law, known as *Shari'ah* Law, also enforces notions of privacy, under which individuals must be compensated for damages resulting from the disclosure or seizure of private information.

The United States (US) recognized Saudi Arabia's efforts to enhance cyber safety and other business protections by removing the kingdom from the Special 301 Report in 2010, 2011, 2012 and 2013, recognizing "Saudi Arabia's success in improving its IP rights protection and enforcement regime."[97] The 2010 Special 301 Report elaborated, "enforcement, prosecutions, and transparency issues were successfully addressed in the past year, and the US will continue to engage with Saudi Arabia to address remaining issues."[98] Not only do these developments improve cyber defense, they also provide much needed protection and reassurance for foreign firms considering business in Saudi Arabia.

---

[85] (Baker & McKenzie Ltd, 2012).
[86] *Ibid.*
[87] *Ibid.*
[88] *Ibid.*
[89] (Saudi Arabia General Investment Authority).
[90] *Ibid.*
[91] (El Farag, 2012).
[92] (WIPO, 2013).
[93] *Ibid.*
[94] (KSA, Anti-Cyber Crime Law, 2007).
[95] *Ibid.*
[96] (Al-Bosaily, 2011).
[97] (El-Farag, 2012).
[98] (Trade Representative, 2013).

TAXATION

Saudi Arabia's corporate income tax system subjects foreign firms (non-GCC members) to a flat 20 percent levy. If a company is a joint venture between Saudi Arabian and foreign parties, the foreign party's income from the venture is subject to the applicable foreign tax rate, and the Saudi Arabian party's income is subject to a 2.5 percent religious tax called *zakat*, which is the typical rate levied upon Saudi Arabian corporations.[99]

Saudi Arabia's corporate tax system is highly regarded for its simplicity and clarity. According to the World Bank's Doing Business 2013 report, Saudi Arabia ranks third among 185 countries surveyed in terms of ease of paying taxes.[100] This rank increased from tenth place in 2012.[101] Additionally, the World Bank report notes that Saudi Arabia "ranks among the 10 economies with the fewest payments and lowest tax compliance time."[102] In 2011, the Saudi Arabian government implemented an electronic filing system to provide further efficiencies to the tax process. However, KPMG, a US-based accounting firm, reported that serious bugs remain in the system, and recommended that foreign firms make physical payments and continue to take paper receipts until the electronic system is stabilized.[103]

For more information on Saudi Arabia's IP and cyber security-related laws, refer to the following resources:

- Law of Trademarks
- Law of Patents, Layout-Designs of Integrated Circuits, Plant Varieties, and Industrial Designs
- Copyright Law
- Law of Trade Names
- Anti-Cyber Crime Law

POLITICAL ENVIRONMENT

The Kingdom of Saudi Arabia's (Saudi Arabia) political regime has demonstrated relative stability in recent decades, boding well for foreign firms considering doing business in this foreign market. Saudi Arabia has been governed by a monarchy since the kingdom was first formed in 1932.[104] Since his ascension to power in 2005, King Abdullah bin Abdul Aziz has undertaken social and economic reforms, and experienced considerable growth.

Islam sits at the core of the governance of Saudi Arabia, with conservative religious values driving much of the decision-making in the political, legislative and legal systems.[105][106] Foreign firms should be aware that the monarchy and the values of Islam play a key role in shaping the political agenda. Although the kingdom may not offer the democratic institutions that western corporations are accustomed to, it does appear to maintain a high degree of permanence. Therefore, Saudi Arabia is a politically stable market. In

[99] (EIU, Corporate Tax, 2013).
[100] (World Bank, Doing Business).
[101] (EIU, Saudi Arabia Regulation Overview).
[102] (World Bank, Doing Business).
[103] (KPMG, 2012).
[104] (Cordesman, 2011).
[105] (Latham & Watkins, 2010)
[106] (Cordesman, 2011).

addition to the political climate, the overall environment in the kingdom has become more stable and secure.[107] Still, the presence of terrorists groups pose threats to security.[108]

Recognizing its vulnerability to cyber-attacks, especially considering its vast energy resources and networks, Saudi Arabia's government has participated in several international agreements to mitigate cyber threats and enhance cyber security.[109]

For more information on Saudi Arabia's political environment, refer to the following resource:

- CSIS Report on Saudi Arabian Stability
- Economist Intelligence Unit's Political Structure Summary
- Department of State's Saudi Arabian Travel Information

ECONOMIC ENVIRONMENT

Saudi Arabia possesses a prosperous economy and offers a competitive market, both relative to the region and the globe. It ranks relatively high among global gross domestic product (GDP) output, and maintains the highest GDP in the Middle East region. The GDP in 2011 totaled approximately $576.8 billion, and jumped to $711 billion in 2012.[110] The economic growth in the country has consistently increased in recent years. From 2008 to 2012, real GDP increased at a rate of 6.2 percent.[111] Trade accounted for a remarkable 92.3 percent of GDP from 2009 to 2011.[112] In addition to trade, much of the growth in the economy has been led by government spending, which bodes well for US defense firms marketing to the military and other government agencies.[113] The economic environment is ripe for foreign firms and other market entrants.

For additional information on Saudi Arabia's economy, refer to the following resources:

- World Trade Organization Member Profile on the Kingdom of Saudi Arabia

SOCIO-CULTURAL ENVIRONMENT

Given that Saudi Arabia is an Islamic Monarchy, there are many cultural considerations that western firms should take into consideration. Gender inequality and censorship are arguably the most significant cultural features; both are heavily motivated by religious conservatism. In addition, the influence of *Shari'ah* law is another manifestation of the role of Islam, and a business condition that is unique to Saudi Arabia.

[107] (Department of State).
[108] *Ibid.*
[109] (GAO, 2010).
[110] (WTO, 2013).
[111] (EIU, Fact Sheet, 2013).
[112] (WTO, 2013).
[113] (EIU, Long-term Outlook, 2013).

GENDER INEQUALITY

Foreign firms must be sensitive to gender inequality norms in the kingdom. In Saudi Arabia women are denied many fundamental rights including education, employment, health, suffrage, and equal legal protection.[114] Female employment is severely restricted and requires the supervision of a male guardian.[115] Furthermore, women must be physically segregated in the workplace. [116] Notwithstanding, Saudi Arabia appears to be making strides towards improving the treatment of women. Foreign firms with female leadership and/or a predominantly female workforce may find it difficult to contract with the government.

CENSORSHIP

Censorship may pose a challenge, or at least a limitation, for foreign firms. Regardless, all foreign firms should be aware of the informational limitations. In 2013, Saudi Arabia ranked 163th out of 179 countries on the World Press Freedom Index.[117] Rigid censorship laws are enforced in Saudi Arabia. The framework for media regulation and enforcement was augmented in 2011.[118] Saudi Arabia also conducts social media monitoring. Earlier in 2013, services that refused to provide access to social media content were no longer allowed to operate domestically.[119] While these constraints may pose an obstacle to certain market entrants, they may also present an opportunity for companies offering monitoring services.

DOING BUSINESS

Saudi Arabia ranks relatively high for business indicators, reflecting a supportive business climate, outside of the aforementioned social constraints. The World Bank ranked Saudi Arabia 22nd out of 185 countries for ease of doing business in 2013. Saudi Arabia generally maintains western limited liability corporation (LLC) formation standards and rights.[120] Saudi Arabia maintains strong disclosure requirements and other provisions to ensure investor protection in business transactions.[121] Contract enforcement ratings in Saudi Arabia exceed the Middle East and North African averages, and are somewhat competitive with Organization for Economic Cooperation and Development (OECD) countries.[122] Although timelines to resolve insolvency are reasonable and relatively short, there is a very low bankruptcy recovery rate of 28 percent of investment in Saudi Arabia.[123] Overall, Saudi Arabia offers a competitive business climate for foreign firms, especially considering the market opportunities available.

PIRACY

Despite a relatively comprehensive IP regime, piracy remains a major problem in Saudi Arabia. According to the Business Software Alliance's 2011 Global Software Piracy Study, software was pirated at a rate or 51 percent in 2011.[124] In the US, the average piracy rate is less than half that of Saudi Arabia's at 19 percent.[125] Foreign firms bringing valuable software into the private and consumer markets in Saudi Arabia would need to be cautious of this threat.

---

[114] (HRW, 2008).
[115] *Ibid.*
[116] *Ibid.*
[117] (Reporters Without Borders, 2013).
[118] (EIU, Saudi Arabia Internet, 2013).
[119] *Ibid.*
[120] (Latham & Watkins, 2010).
[121] (World Bank, Doing Business, 2013).
[122] *Ibid.*
[123] *Ibid.*
[124] (EIU, Software, 2013).
[125] *Ibid.*

SHARI'AH LAW

Notably, much of Saudi Arabia's legal system is governed or guided by *Shari'ah* Law.[126] King Abdullah passed a new Law of Judiciary in 2007 to establish separate commercial and labor courts for the private sector. [127] These reforms have not yet been implemented, but once implemented will increase the ease of doing business in the kingdom.[128]

For more information on Saudi Arabia's business climate, please refer to the following resource:

» World Bank's Doing Business Assessment of Saudi Arabia

DEMAND FROM PRIVATE SECTOR

In addition to public demand, there is clearly a role for private sector cyber security exports. The US trade mission to Saudi Arabia in September also identified opportunities in the private sector.[129] Energy companies, especially in Saudi Arabia, are often targets of cyberattacks given their close proximity to energy infrastructure, role in the domestic economy, and linkages to the oil revenues that fund the government.

Private financial institutions, technology firms, communications companies and transportation providers are also likely to invest in cyber security. In 2013, the Saudi Airlines spent more than $10 million on cyber security. During the same year, King Abdulaziz's City for Science and Technology spent more than $12 million. Mobily, Saudi Arabia's fastest growing telecommunications provider, recently partnered with IBM to reinforce its technical infrastructure and implement new technologies to ease development.[130] Similar opportunities for partnerships with major Saudi Arabian companies exist for new market entrants.

In an empirical study, 164 respondents out of 167 respondents from private firms confirmed that their organization was focused on enhancing IT security.[131] It is clear that the vast majority of private sector firms in Saudi Arabia have already or plan to ramp up investment in cyber security, suggesting that the demand for cyber security imports in the private sector is nearly as large as the government's demand.

[126] (Latham & Watkins, 2010).
[127] *Ibid.*
[128] *Ibid.*
[129] (International Trade Administration, 2013).
[130] (IBM, 2012).
[131] (Abu-Musa, 2010).

Table 1: Saudi Arabia Cyber Security Market at a Glance

Strengths

- High defense spending of over $56b
- Government recognition of the need for cyber security
- Close defense relationship with USA

Weaknesses

- Cultural and institutional differences due to which agents might be necessary

Opportunities

- Public and private sector opportunities in information technology
- Surveillance technology, cyber intrusion prevention, detection equipment, etc.

Threats

- Competition from global technology companies already engaged in the UAE market

APPENDIX 1: USEFUL LINKS

- Anti-Cyber Crime Law
- CIA World Factbook Analysis of Saudi Arabia
- Commercial Service Report on Saudi Arabia
- Communication and Information Technology Commission Public Consultation Solicitation Page
- Congressional Research Service Report on Saudi Arabian Background and US Relations
- Copyright Law
- CSIS Report on Saudi Arabian Stability
- Department of State's Saudi Arabian Travel Information
- Economist Intelligence Unit Fact Sheet on Saudi Arabia
- Economist Intelligence Unit Long-Term Economic Outlook for Saudi Arabia
- Economist Intelligence Unit's Political Structure Summary
- Global Tenders
- Information Technology Tenders
- ITA Trade Mission to Saudi Arabia
- Kingdom of Saudi Arabia Tenders
- Law of Patents, Layout-Designs of Integrated Circuits, Plant Varieties, and Industrial Designs
- Law of Trade Names
- Ministry of Defense
- Ministry of Finance Tenders List
- Saudi Arabia's Draft National Information Security Strategy
- Saudi Arabia's government website on trade agreements
- Saudi Arabian General Investment Authority
- Saudi Tenders
- Technical Cooperation Agreement between the US and Saudi Arabia
- TIFA Agreement between the US Government and the Kingdom of Saudi Arabia
- Umm Al-Qura Gazette
- USTR analysis of trade barriers in Saudi Arabia
- World Bank's Doing Business Assessment of Saudi Arabia
- WTO Member Profile on the Kingdom of Saudi Arabia

APPENDIX 2: GOVERNMENT CONTACTS

- **Communication and Information Technology Commission** (CITC), PO Box 75606, Riyadh 11588; tel: (966.1) 461-8020; fax: (966.1) 461-8000; internet: http://www.citc.gov.sa.
- **King Abdul Aziz City for Science and Technology** (KACST), PO Box 6086, Riyadh 11442; tel: (966.1) 488-3555; fax: (966.1) 488-3118; internet: http://www.kacst.edu.sa/en/Pages/default.aspx.
- **Ministry of Finance**, Airport Road, Riyadh 11177; tel: (966.1) 405-0000; fax: (966.1) 405-9202; internet: http://www.mof.gov.sa.
- **Saudi Aramco**, PO Box 5000, Dharan Airport 31311; tel: (966.3) 876-5229; fax: (966.3) 876-6520; internet: http://www.saudiaramco.com/en/home.html.
- **Saudi National E-Government Portal**, King Abdul Aziz Communication Complex, Al-Morsalat Quarter, Riyadh 11112; internet: http://www.saudi.gov.sa.
- **Saudi Electronic Data Interchange** (SaudiEDI), P.O. Box 221630 Riyadh 11311; tel: (966.1) 477-4488 Ext: 1 or 2; fax: (966.1) 473-3834; email: customer@saudiedi.com; internet: http://www.saudiedi.com.
- **Deputy Prime Minister, Ministry of Defense, HRH Crown Prince Salman bin Abdulaziz Al-Saud,** Airport Road, Riyadh 11165; tel: 1-478-5900/1-477-7313; fax: 1-401-1336.
- **Ministry of Industry**, PO Box 5729, Riyadh 11127 (Omar bin Al-Khatab Road; N. of Rail Station); tel: 1-477-2722/1-477-6666; fax: 1-477-5451,
- **Ministry of Interior,** PO Box 2933, Riyadh 11134 tel: 1-401-1944; fax: 1-403-1185; internet: http://www.moi.gov.sa.
- **Ministry of Planning and National Economy**, PO Box 1358, University Street, Riyadh 11183; tel: 1-402-3562/1-401-3333; e-mail: info@cds.gov.sa; internet: http://www.planning.gov.sa/.

Chambers of Commerce

- **Council of Saudi Arabian Chambers of Commerce and Industry**, PO Box 16683, Riyadh; tel: (966.1) 405-3200; fax: (966.1) 402-4747; internet: http://www.saudichambers.org.sa.
- **Eastern Province Chamber of Commerce and Industry**, PO Box 719, Dammam; tel: (966.3) 857-1111; fax: (966.3) 833-5755; internet: http://www.chamber.org.sa.
- **Federation of GCC Chambers of Commerce**, PO Box 2198, Dammam; tel: (966.3) 826-5943; (966.3) 826-6974; internet: http://www.fgccc.org.
- **Jeddah Chamber of Commerce and Industry**, PO Box 1264, Jeddah; tel: (966.2) 651-5111; fax: (966.2) 651-7373; internet: http://jcci.org.sa.
- **Riyadh Chamber of Commerce**, PO Box 596, Riyadh; tel: (966.1) 404-0044; fax: (966.1) 402-1103; internet: http://www.riyadhchamber.com/index.php.
- **US-Saudi Arabian Business Council**, 1401 New York Avenue NW, Washington DC 20005; tel: (1.202) 638-1212; fax: (1.202) 638-2894; internet: http://www.us-sabc.org.

Source: Economist Intelligence Unit, Saudi Electronic Data Interchange, Royal Embassy of Saudi Arabia

APPENDIX 3: EXAMPLES OF CYBER SECURITY RELATED TENDERS

Organization or Industry	Project Description	Deadline
Information Technology (IT)	Project of Application of Financial and Administrative System (ERP System) for Security Forces	12/24/2013
Information Technology	Improvement Project and the Development of System Resources MOI-Expand.	12/9/2013
Information Technology	Establishment, Operation and Maintenance of Electronic System	12/25/2013
Telecommunications/Infrastructure/IT	Construction of Infrastructure for Information Technology	12/17/2013
Telecommunications/Infrastructure/IT	Network and Information Security Infrastructure Project	Not specified
Information Technology	Security & Protection System Installation	Not specified
Information Technology	Infrastructure for IT, King Fahd Industrial Ports	12/18/2013

Source: Global Tenders

REFERENCES

About Saudi Arabia: Government. (2013). Royal Embassy of Saudi Arabia. http://www.saudiembassy.net/about/country-information/government/.

Abu-Musa, Ahmad (2010). . Information security governance in Saudi organizations: An empirical study. *Information Management & Computer Security* 18.4: 226-76. *ProQuest.* Web. http://search.proquest.com.mutex.gmu.edu/docview/761419954?accountid=1454 .

Ageli, Mohammed Moosa, and Shatha M. Zaidan. (2013). Consequential effects of defence expenditure on economic growth of Saudi Arabia: 1970-2012. *International Journal of Economics and Finance* 5.2 (2013): 155-63. *ProQuest.* Web. 12 Oct. 2013.

Al-Bosaily, Abdulaziz. (2011). Data Protection Update 5 - Data Protection in The Kingdom Of Saudi Arabia. *Mondaq Business Briefing*. May 2011, Print.

An Outline of Various Forms of Doing Business in Saudi Arabia. (2012). *Baker & McKenzie Ltd.* Legal Advisors. April 2012. Print. http://www.bakermckenzie.com/files/Publication/bc8702e2-20bc-4d91-8c61-7c16d910a3cf/Presentation/PublicationAttachment/7c7f008a-b98d-4d3c-9cce-7dee4b2034dd/bk_saudiarabia_dbi_12.pdf .

Central Intelligence Agency. Saudi Arabia. *The World Factbook*. Central Intelligence Agency, n.d. Web. https://www.cia.gov/library/publications/the-world-factbook/geos/sa.html.

Chun, Clayton K.S. (2010). Do oil exports fuel defense spending? *Strategic Studies Institute*. Feb. 2010, Print.

Cordesman, Anthony H. (2003). Saudi Arabia Enters the Twenty-First Century: The Political, Foreign Policy, Economic, and Energy Dimensions. Praeger Security International Online. Westport, CT: Praeger Publishers. Web. http://psi.praeger.com/doc.aspx?adv_search=1&term_0=Saudi+Arabia&index_0=place&op_1=AND&term_1=cyber+security&index_1=words&op_2=AND&term_2=&index_2=words&op_3=AND&term_3=&index_3=words&s=r&freeform=&d=/books/dps/200094ab/200094ab-p200094ab9970041001.xml&i=0.

Cordesman, Anthony H. (2011). Understanding Saudi Stability and instability: A very different nation. *Center for Strategic and International Studies*. 26 Feb 2011. Web. http://csis.org/publication/understanding-saudi-stability-and-instability-very-different-nation.

Cordesman, Anthony, H. and Nawaf Obaid. (2204). Saudi Internal Security: A risk assessment. *Center for Strategic and International Studies*. May 2004. Print. http://csis.org/files/media/csis/pubs/sis_ariskassessment.pdf.

Crowell.com, (2013). So you want to do business with the Saudi Government. Crowell.com. Crowell Moring. Print. http://www.crowell.com/files/So-You-Want-to-Do-Business-with-the-Saudi-Government-Crowell-Moring.pdf.

Dehaas, Josh. (2011). A Crackdown On Bloggers. *Maclean's* 124.3 36. *Readers' Guide Full Text Mega (H.W. Wilson)*. Web. http://pc6bf4sj5m.search.serialssolutions.com/log?L=PC6BF4SJ5M&D=ESX&J=MACLTO&P=Link&U=http%3A%2F%2Fmutex.gmu.edu%2Flogin%3Furl%3Dhttp%3A%2F%2Fopenurl.ebscohost.com%2Flinksvc%2Flinking.aspx%3Fgenre%3Darticle%26issn%3D0024-

9262%26date%3D2011%26volume%3D124%26issue%3D3%26spage%3D36%26atitle%3DA%2Bcrackdown%2Bon%2Bbloggers.%26aulast%3DDehaas

Doing Business 2013: Saudi Arabia. (2013). *The World Bank*. Web. http://www.doingbusiness.org/data/exploreeconomies/saudi-arabia/.

Doing Business in Saudi Arabia: 2011 Country Commercial Guide for U.S. Companies. *US Department of State.* 2011. Web. http://export.gov/saudiarabia/static/CCG_Latest_eg_sa_056382.pdf.

Doing Business in Saudi Arabia. *Latham & Watkins*. May 2010. Web. http://www.lw.com/upload/pubcontent/_pdf/pub3507_1.pdf.

Economist Intelligence Unit. (2013). All-female BPO centre to be created. *Country Profiles and Country Commerce: Economy Forecast*. EIU, Sept. 2013. Web. http://country.eiu.com.mutex.gmu.edu/article.aspx?articleid=301006814&Country=Saudi%20Arabia&topic=Economy&subtopic=Forecast&subsubtopic=Policy+trends&u=1&pid=1290975313&oid=1290975313&uid=1.

Economist Intelligence Unit. (2013). Data Tool. *EIU*Web. http://data.eiu.com.mutex.gmu.edu/EIUTableView.aspx?geography_id=470000047&pubtype_id=1393181324.

Economist Intelligence Unit. (2012). Investigation blames non-Saudis for Aramco cyber-attack. *Country Profiles and Country Commerce*. EIU, Dec. 2012. Web. http://country.eiu.com.mutex.gmu.edu/article.aspx?articleid=1389925323.

Economist Intelligence Unit. (2013). Saudi Arabia Country Report: Fact Sheet. *Country Profiles and Country Commerce*. EIU, 2013. Web. http://country.eiu.com.mutex.gmu.edu/article.aspx?articleid=840973668&Country=Saudi%20Arabia&topic=Summary&subtopic=Fact+sheet.

Economist Intelligence Unit. (2013). Saudi Arabia Country Report: Long-term outlook. *Country Profiles and Country Commerce*. *EIU*. Web. http://country.eiu.com.mutex.gmu.edu/article.aspx?articleid=1450755729&Country=Saudi%20Arabia&topic=Economy&subtopic=Long-term+outlook&subsubtopic=Summary.

Economist Intelligence Unit. (2013). Saudi Arabia Country Report: Overview of e-commerce. *Industry: Telecommunications*. *EIU*, June 2013. Web. http://country.eiu.com.mutex.gmu.edu/ArticleIndustry.aspx?articleid=1010712485&Country=Saudi%20Arabia&topic=Industry&subtopic=Telecommunications.

Economist Intelligence Unit. (2013). Saudi Arabia Internet: Quick view - Saudi leadership seeks to crack down on social media. *EIU*, April 2013. Web. http://country.eiu.com.mutex.gmu.edu/ArticleIndustry.aspx?articleid=360341020&Country=Saudi%20Arabia&topic=Industry&subtopic=Telecommunications.

Economist Intelligence Unit. (2013). Saudi Arabia Regulation Overview: Corporate Tax. *Country Profiles and Country Commerce*. EIU. (2013).

Economist Intelligence Unit. (2013). Saudi Arabia risk: Alert - Interior ministry warns of cyber attack. Risk Briefing. *EIU*, 11 Sept. 2013. Web. http://viewswire.eiu.com.mutex.gmu.edu/index.asp?layout=RKArticleVW3&article_id=370946221.

Economist Intelligence Unit. (2013). Saudi Arabia software: Sub-sector update. *Saudi Arabia Industry*. *EIU*. Feb. 2013. http://country.eiu.com.mutex.gmu.edu/ArticleIndustry.aspx?articleid=1760217960&Country=Saudi%20Arabia&topic=Industry&subtopic=Telecommunications.

El Farag, Mohamed Salem Abou. (2012). What is new in the United States Trade Representative's Special 301 Report for Arab Countries? *The International Lawyer* 46.2 683-90. *ProQuest.* Web. http://search.proquest.com.mutex.gmu.edu/docview/1220741525/fulltext?accountid=14541.

Growing pains for Saudi Arabia's withholding tax. (2012). KPMG *International Cooperative*. Nov 2012.

Human Rights Watch. Perpetual minors: Human rights abuses stemming from male guardianship and sex segregation in Saudi Arabia. (2008). *HRW*. April 2008. Web. http://www.hrw.org/print/reports/2008/04/19/perpetual-minors.

International Business Machines (2012). Mobily Taps IBM for business transformation in agreement valued at about $280 million. *IBM, News Release*. Aug. 2012. Web. http://www-03.ibm.com/press/us/en/pressrelease/38553.wss.

Kingdom of Saudi Arabia. Bureau of Experts at the Council of Ministers. (2007). Anti-Cyber Crime Law (8 Rabi 11428 / 26 March 2007). *Royal Decree No. M/17*, March 2007. Web. http://www.saudiembassy.net/announcement/announcement03260701.aspx.

Kingdom of Saudi Arabia. (2013). General Investment Authority. *Corporate Income Tax*. Riyadh, 2013. Print.

Kingdom of Saudi Arabia. (2012). Ministry of Communications and Information and Technology. Developing a national information security strategy in Saudi Arabia: Public Comment Document. *MCIT Pubic Consultations*. Web. http://www.mcit.gov.sa/english/Pubreg/NationalCenter_01_en.htm.

Naseba. (2013). About the summit. *Digital Security Summit*: Web. http://www.digitalsecuritysummit.com/about/summit/.

Knickmeyer, Ellen. (2013). After cyberattacks, Saudi steps up online security. *Wall Street Journal*. New York. 26 Aug. 2013. Web. http://blogs.wsj.com/middleeast/2013/08/26/after-cyberattacks-saudi-steps-up-online-security/.

Naseba. (2013). About the summit. *Digital Security Summit*: Web. http://www.digitalsecuritysummit.com/about/summit/.

Reporters Without Borders (2013). World Press Freedom Index. *RWP* Web. http://en.rsf.org/press-freedom-index-2013,1054.html

Research and markets: Saudi Arabia - Telecoms, mobile, broadband and forecasts. *M2 Presswire*. Apr 18 2012. *ProQuest.* Web. http://search.proquest.com.mutex.gmu.edu/docview/1001888890/abstract?accountid=14541#center.

Roberts, John. (2012). Cyber threats to energy security, as experienced by Saudi Arabia. Platts, McGraw Hill Financial. Nov 2012. Web. http://blogs.platts.com/2012/11/27/virus_threats/.

Saudi e-Government Program. Best practices of IT procurement. 2009. http://www.yesser.gov.sa/en/Methodologies/Pages/best_practices_government.aspx

Saudi Arabia country snapshot. *FedEx*. 2013. Web. https://smallbusiness.fedex.com/international/country-snapshots/saudi-arabia.

Saudi Arabia. Government tenders and procurement. *Royal Decree No. M/58, 27* September 2006. Print. http://goo.gl/8BcImA.

Saudi Arabia. Implementation of government tender and procurement law. Minister of Finance Decision No. 362, 10 March 2007. http://goo.gl/4kJiqy.

Saudi Arabia. Ministry of Foreign Affairs. His Royal Highness Prince Salman bin Abduaziz Al-Saud. Feb 2012, Web. http://www.mofa.gov.sa/sites/mofaen/aboutkingdom/saudigovernment/saudileadership/pages/leadership234437.aspx.

Saudi Arabia. Saudi Arabia General Investment Authority. SAGIA Business Center: Legal business structures in the kingdom. n.d. (2013) http://www.sagia.gov.sa/Documents/Wizard/Legal_Structure.pdf .

Saudi Aramco. Our Company. (2013). Web. http://www.saudiaramco.com/en/home.html#our-company%257C%252Fen%252Fhome%252Four-company.baseajax.html.

Shanker, Thom and Sanger, David E. (2013). U.S. helps allies trying to battle Iranian hackers. *New York Times*. 8 Jun 2013. Web. http://www.nytimes.com/2013/06/09/world/middleeast/us-helps-allies-trying-to-battle-iranian-hackers.html?_r=0.

Stockholm International Peace Research Institute. (2013). Military expenditure data by Country. *SIPRI*, Web. http://portal.sipri.org/publications/pages/expenditures/country-search.

The World Bank. (2012) Internet Users (per 100 people). *The World Bank*, Web. http://data.worldbank.org/indicator/IT.NET.USER.P2.

U S Department of Commerce. (2013). Trade mission to Saudi Arabia and Kuwait. *U.S. Commercial Service.* Sept 2013. Web. http://export.gov/kuwait/build/groups/public/@eg_kw/documents/webcontent/eg_kw_065244.pdf.

U S Department of State. (2008) Technical cooperation agreement between the United States of America and the Kingdom of Saudi Arabia. 16 May 2008. Print. Washington D.C.: GPO.

U S Government Accountability Office. (2010) Cyberspace: United States faces challenges in addressing global cybersecurity and governance. *Government Accountability Office*. Print. Washington D.C.: GPO.

U S International Trade Administration. (2013). Critical infrastructure protection and cyber security trade mission to Saudi Arabia and Kuwait. *Federal Register* 78 (31 January 2013) Web. https://federalregister.gov/a/2013-02052.

U S. Trade Representative. (2010) 2010 Special 301 Report. Print. Washington D.C.: GPO.

U S Trade Representative. (2012). Saudi Arabia – Foreign Trade Barriers. 2012. http://www.ustr.gov/sites/default/files/Saudi%20Arabia_0.pdf.

U S Trade Representative. (2003) Middle East Free Trade Area Initiative. http://www.ustr.gov/sites/default/files/uploads/agreements/tifa/asset_upload_file304_7740.pdf.

U S Trade Representative. (2003) Trade and Investment Framework Agreement between the United States of America the Kingdom of Saudi Arabia. http://www.ustr.gov/sites/default/files/uploads/agreements/tifa/asset_upload_file304_7740.pdf.

Woodson, C.A. (1998) Saudi Arabian Force structure development in a Post Gulf War World. *Foreign Military Studies Office*. Fort Leavenworth, KS: June 1998. Web. http://fmso.leavenworth.army.mil/documents/saudi/saudi.htm#app1.

World Intellectual Property Organization. (2013). Saudi Arabia. *WIPO Lex*. WIPO. Web. http://www.wipo.int/wipolex/en/profile.jsp?code=SA#a1.

World Trade Organization. (2013). Member information: Kingdom of Saudi Arabia and the WTO. *Members*. WTO, 2013. Web. http://stat.wto.org/CountryProfile/WSDBCountryPFView.aspx?Language=E&Country=SA.

World Trade Organization. (2007) The Plurilateral Agreement on government procurement. Web. http://www.wto.org/english/tratop_e/gproc_e/gp_gpa_e.htm.