Virginia
ExportVirginia.org
BUSINESS WITHOUT BORDERS

Cyber Security Export Markets

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

PREFACE

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 Virginia Economic Development Partnership, the lead economic development authority for the Commonwealth of Virginia, with financial support from the Office of Economic Adjustment, United States Department of Defense.

This study was conducted by an interdisciplinary team from the graduate International Commerce and Policy Program in the School of Public Policy at George Mason University.

Virginia has been consistently rated by various studies as the best state for doing business in the United States. The industries of information technology and defense are among the major industries within Virginia. The global demand for cybersecurity technology is exploding.

The project identifies the top ten foreign markets that offer the best opportunities for exports of cyber security goods, services and technologies by companies located in Virginia. In addition to providing a broad overview of the top ten markets, the study identifies and analyzes in depth the five most promising markets. The ten markets examined are presented in the order of the most promising. The first five contain the in-depth assessments. These assessments focus on strategies for market access, including government procurement procedures, trade regulations, laws, market access restrictions, tenders, and business challenges.

TEAM MEMBERS

Stuart Malawer, Principal Investigator (*Distinguished Service Professor of Law and International Trade* at the School of Public Policy, George Mason University).

Arun Sood, Co-Principal Investigator (*Director*, International Cyber Center and *Professor* of *Computer Sciences,* George Mason University).

General Michael Hayden (Retired), Consultant (*Distinguished Visiting Professor* at the School of Public Policy, George Mason University, formerly *Director* of the National Security Agency and the Central Intelligence Agency).

Sonia Ketkar, Director of this study (*Assistant Professor* at the School of Public Policy, George Mason University).

Hollis Beckner (International Commerce and Policy Program, School of Public Policy, George Mason University).

Victoria Huttar (*Graduate* of the International Commerce and Policy Program, School of Public Policy, George Mason University).

Katie Praske (*Graduate* of the International Commerce and Policy Program, School of Public Policy, George Mason University).

REPORT ON CYBER SECURITY

INTRODUCTION

The Stockholm International Peace Research Institute (SIPRI) noted that, "the traditional arms producers and military services companies that have expanded their cybersecurity business provide security professionals (in the military, intelligence and law-enforcement communities) with products and services designed for offensive operations in cyberspace—developing cyberweapons and network attack strategies; looking for undiscovered vulnerabilities in hardware and software (so-called zero-day vulnerabilities); and surveillance and espionage services. Alongside these are products and services—such as network and data protection software; testing and simulation; and training and consulting—that are designed to protect networks and information systems or make them more resilient to cyberattacks."(Boulanin, 2013)

This quote from SIPRI sums up the nature of the global cyber security industry. Its players include national governments, large multinational companies, smaller sized suppliers and even individual consumers who need security while browsing the Internet in their homes or offices. Cyber security is a growing industry, the relevance of which is expected to increase in the coming years as every country in the world becomes more cyber-dependent. This trend has created plenty of opportunities for cyber security companies in Virginia to export their products and services. In this report, we identify the top export markets for the Commonwealth's cyber security industry.

In some ways, the growth of the cyber security industry mirrors that of the defense industry comprised of the army, the navy and the air force. Thus, the countries which appear as the top markets for cyber security exports are indeed those that are also top markets for defense exports from the United States – that is the Middle Eastern Gulf nations of Qatar, Kuwait, Saudi Arabia, and the United Arab Emirates. Since the economy in these nations is majority-controlled by the government, the government, often through the defense ministries, also determines cyber security expenditures.

In more democratic markets such as the United Kingdom or Australia, cyber security programs and initiatives are shared by the public and the private sector, which also manages national infrastructure in these economies.

TOP 10 MARKETS FOR CYBER-SECURITY EXPORTS

A well-publicized report released by Markets and Markets Research in January 2013 notes that the largest cyber-security market is North America ($93.6 billion), followed by Europe ($24.7 billion), Asia-Pacific ($23.2 billion), the Middle East ($22.8 billion) and Latin America ($1.6 billion). The purpose of this report, however, is to identify the top ten individual country markets for exporting cyber security related products and services from the United States (US) with a focus on foreign government contracts rather than broad regions. After thorough research using primary and secondary sources, the list is below.

METHODOLOGY FOR IDENTIFYING TOP 10 MARKETS

The conditions for including country markets on the list are (1) US export controls and trade regulation, (2) market potential as indicated by government plans, expenditures on cyber security as well as demand for cyber security products and services, and (3) market growth in the immediate future.

US EXPORT CONTROLS AND TRADE REGULATION

Due to the sensitive nature of defense or security exports, we first referred to the Commerce Control List (CCL) and the US Munitions List (USML) to identify the countries to which US exports are restricted or

embargoed. Some export items in the defense or security category are subject to mandatory licenses and other procedures. This is especially true in the case of exports to those nations on our list that are not NATO members, Japan or Australia. This process of examining trade policies and regulation yielded a long list of countries to which American firms can potentially export their products after government approvals.

PROCESS OF SELECTING AND ELIMINATING MARKETS

In the next stage, we evaluated demand in the list of available markets based on the following factors - government spending on defense and cyber security initiatives and programs; incidents of cyber-attacks; existence and nature of cyber security policy and systems; trade; defense and political relations with the United States; presence of multinational firms and the interest of the domestic private sector in undertaking expenditures to secure their operations; among other such factors which we believe are crucial in evaluating the opportunities in this sector in any foreign market. We also took into consideration the availability or lack thereof of cyber security expertise in the given market. We paid particular attention to the market potential and demand in nations that had an existing free trade agreement or a defense trade cooperation agreement (United Kingdom and Australia) or a defense cooperation agreement (Brazil) with the United States[1]. Additionally, we consulted with General Michael Hayden, former Director of the National Security Agency and former Director of the Central Intelligence Agency for guidance.

We would like to clarify that there are other national markets, which were not included on our list but are indeed destinations for cyber security related exports from the United States. Since we included only the 'top' ten, we focused on identifying those markets which our research indicated were 'relatively' more promising and had higher potential than the other countries.

THE TOP TEN (10) MARKETS[2]

1. THE KINGDOM OF SAUDI ARABIA (SAUDI ARABIA)

According to various reports, the cyber security market in Saudi Arabia is expected to grow 30 percent by 2016 to $37.5 billion. In spite of its plentiful energy resources, there are very few domestic firms that can supply its cyber security needs. It is known that companies and countries specializing in the energy sector are popular targets for cyber-attacks. For example, Saudi Arabia's Aramco was the victim of attacks at the end of 2012. The goal of the attack was to disrupt the world energy market. There is also considerable discussion that most foreign multinationals with a presence in the Middle Eastern countries have encountered significant security breaches. The interdependencies among the geographically dispersed units of a multinational company make the threat even more acute. In June 2013, the US started providing support to Saudi Arabia to strengthen its cyber security defenses (Shanker & Sanger, June 2013).

2. THE UNITED ARAB EMIRATES (UAE)

The UAE has experienced an increasing number of cyberattacks each year (Al Makaleh, 2013) Symantec predicted that the UAE would continue to be targeted in the coming years (Hafeez, 2011). Along with the other GCC nations of Saudi Arabia, Qatar, Kuwait and Oman, the UAE is gearing up to increase its spending on cyber security. In June 2013, the US started providing support to the UAE also to strengthen its cyber security defenses (Shanker & Sanger, June 2013).

---

[1] The United Kingdom and Australia benefit from a special treaty with the United States under which certain products are exempt from ITAR restrictions. More details can be obtained from http://pmddtc.state.gov/treaties/index.html

[2] It is difficult to obtain exact spending figures and budget details for the Middle Eastern countries because their governments often do not publish this information. Therefore, our ranking was based on qualitative information about the market potential and access in these countries.

3. QATAR

In the year 2012, Qatar had one of the highest per capita incomes in the world making it a suitable target for cyber security attacks. To build up its defenses, Qatar revealed its plan to set up a cybersecurity system in early 2013. The government is expected to increase spending on various cyber security projects in the coming years (Qatar's National ICT Plan 2015). Qatar is investing in infrastructure in preparation for the FIFA World Cup in 2022. Cyber security initiatives are expected to be a significant part of this expenditure.

4. KUWAIT

Kuwait formed a partnership with the United Kingdom (UK) in late 2012 for the UK to provide cyber security expertise. Thus, Kuwait expects to use technology developed by the UK to secure its cyber borders. Nevertheless, there is opportunity for American exporters in the immediate future to tap into the Kuwaiti market. As mentioned earlier, the US International Trade Administration led trade missions to Kuwait in 2013 for this purpose. Global consulting giants Booz, Allen, Hamilton and SAIC are looking to hire security experts in Kuwait – a need that Virginia firms can fulfill.

5. SOUTH KOREA

South Korea is a leading market for cyber security exports for the following reasons: (1) the nation has economic and political partnerships with the US including a recently effective free trade agreement. It is a major defense and trade partner; (2) the government plans to invest $8.7 billion on cyber security systems in the years leading up to 2017. It is not only establishing a new department specifically for cyber security but is also looking to develop its capabilities for cyber warfare and to train its employees to respond to cyberattacks (Kolendo, 2013). It recently signed a memorandum of agreement with Microsoft to access the company's expertise for this purpose. American products are viewed positively in South Korea; (3) Representatives from South Korea and the US met in July 2013 to strengthen cooperation on issues of cyber security. The US State Department is looking to deepen this relationship. Furthermore, South Korea's diversified industries provide ample fodder for attacks as well as means for their prevention. Sharing a border with North Korea, which is known to be a perpetrator of cyberattacks, South Korea will continue to be exposed to cyber risks in the foreseeable future.

6. BRAZIL

Recognizing the need for enhanced security against cyberattacks, the Brazilian government invested $40 million in 2013 alone toward this cause (Organization of American States, 2013). Interesting enough, the Brazilian energy company Petrobras is also allocating $9.4 billion over five years toward this purpose. The upcoming football World Cup (FIFA) in 2014 and the Olympics in 2016 serve as additional reasons due to which the Brazilian government is focusing on strengthening its surveillance system. Brazil recently signed an agreement with Argentina to jointly develop cyber security defense systems. Because of the increasing need for expertise on cyber security, there are opportunities in this market in the coming years in Brazil. The country has already seen a trend of venture capitalist funding related to information technology with some emphasis on cyber security.

7. JAPAN

In June 2013, the Japanese government adopted a cybersecurity strategy for the first time after experiencing repeated attacks. However, the nation does not have adequate capacity to fight off severe attacks. A Forbes article (Miller, 2013) claimed that "Japan is short of 80,000 technical experts, whereas the country has about 265,000 experts and 160,000 of them need further education or training". There are similar reports in the press regarding Japan's level of preparedness for cyberattacks that echo the idea (Kallender-Umezu, 2013). Japan and the US are engaged in bilateral strategic discussions on the issue of cyber security.

8. UNITED KINGDOM

The UK government made cyber security a priority in its programs and allocated 650 million pounds sterling (approximately $1 billion) to build capabilities, protect infrastructure and combat cybercrime. The government is also involving the private sector in its initiatives as it sees a rising number of attacks. According to the BBC (Lee, 2012), around 80 percent of the UK's infrastructure is managed by private firms. The UK also has a Defense Trade Cooperation Treaty with the United States and is a strategic partner. The UK provides many opportunities for partnerships with Virginia firms.

9. AUSTRALIA

The Australian government is spending upward of $1.31 billion on cyber security until 2020. There are various reports suggesting that the country is not as prepared to combat such crime as Israel, Sweden, or Finland. In the earlier part of the same year, the nation planned to establish a cybersecurity center to boost the government's ability to protect its economy against cybercrime. There are several reports which indicate that Australia does not have sufficient cyber expertise within its workforce. This indicates a need to import expertise from abroad. Australia has a free trade agreement as well as Defense Trade Cooperation Treaty with the US.

10. INDONESIA

Indonesia is so much in need of cyber security expertise that it is seeking support from Estonia and Finland, which are touted to be the most prepared nations against cyber-attacks. Indonesia embarked on the process of establishing its cyber-defense unit fairly recently in 2012. American firms should seek first mover advantages in this market as it quickly emerges with demand for cyber security services. According to Business Monitor International (2013), "Indonesia is forecast to spend about $11.5 billion on defense in 2013, rising to $18.8 billion by 2017."

THE REST OF THE WORLD

In the following sections, we discuss why certain major trading nations did not make it to the list of the top ten markets for cyber security exports.

EUROPE

We expected to find multiple European markets on our list. Possibly because they had a head start or committed sufficient resources, we found that the Nordic countries of **Finland**, **Sweden,** and **Denmark** are amongst the most well prepared for cyber-attacks. **Norway** is not far behind. The nations of **France, Germany, Spain,** and the **Netherlands** are also advanced in implementing their cyber security strategy. **Portugal** launched new programs to strengthen its cyber security system in 2008 and has seen some progress since then. In 2012, its government sought support from Microsoft to continue its efforts to protect itself against cyber-attacks. The Southern European nations of **Italy** and **Greece** have cyber security strategies that are not very well developed in comparison to their Northern European neighbors. We explored these as potential markets because of their need for cyber security expertise to strengthen their existing defense systems. However, because these markets have been on the brink of economic crises, their governments do not have sufficient resources to allocate toward cyber security at this point in time.

The Central and Eastern European countries are known to face constant threats of cyber-attacks from Russia. **Estonia** was crippled by a cyber-attack in 2007. Since then the country has strengthened its infrastructure such that it is now better prepared for any future problems. Estonia also enjoys the reputation of being the NATO front runner on cyber security and offers its expertise to other countries. **Poland** and **Romania** came under serious consideration from us because their security systems are not advanced. Furthermore, they also face the challenge of securing their physical and cyber borders from Russia on their east. However, these governments have not yet made cyber security a priority in their

budgets to the same degree as some of the other nations on our list. For similar reasons as the ones stated here, we excluded **Austria, Hungary** and other European countries from inclusion in the list of top 10 markets.

WEST AND CENTRAL ASIA

According to various websites and newspaper articles, **Russia** is unprepared to deal with cyber-attacks. It is also in need of cyber security expertise. In June 2013, Russia signed an agreement with the United States to establish communication about events related to cyber security. However, due to the current tense political relations between the two nations on multiple issues, we eliminated Russia from our list.

Georgia and the former USSR states are extremely vulnerable to cyber-attacks but suffer from lack of funds and economic problems. Many reports rank **Israel** as the most well prepared nation against such attacks. The country also boasts a large number of advanced domestic companies that provide cyber security solutions.

NORTH AMERICA

Under normal circumstances, **Mexico** might have been a contender on our list. The reasons are that it is one of the least prepared to deal with a cyber-attack. It is also geographically close to the United States and a part of NAFTA, which make it an ideal destination for American exports. However, the Mexican government does not currently have a solid cyber security strategy and the government is focusing on the drug cartels and drugs trade. It might be some time before the government increases its attention and expenditures on cyber security. We eliminated other markets in Latin America for similar reasons.

ASIA PACIFIC

In September 2013, **Vietnam** and the US agreed to expand their defense collaboration in the coming years on various issues including cyber security. The Vietnamese government issued decrees to develop its information security systems. While this might create many opportunities for cyber security companies, the US arms embargo on Vietnam creates some hurdles. For the time being at least, we eliminated Vietnam from our list. We eliminated India and China as suitable markets for similar reasons.

New Zealand introduced its cyber security strategy in 2011. The nation has made considerable progress since then in strengthening its security system. By some accounts, the government needs to spend more funds on additional capability. Although it is an attractive market, we did not consider its market potential to be as high as that of Australia or the other countries on our list.

AFRICA

The last decade saw many African countries build networks and become a part of the cyber world. The nations of Egypt, South Africa, Kenya, Burkina Faso, Morocco, Cameroon, Tunisia, Sudan, Ivory Coast, Ghana, and Mauritius currently have Computer Emergency Response Teams (CERTs). However, for political and economic reasons, we eliminated most African nations from our list. The only market that might have qualified is **South Africa** because it is more advanced in its use of online technology and more developed in its efforts at cyber security. However, the country is still in the process of developing a full-fledged strategy related to cyber security.

UPCOMING MARKETS FOR CYBER SECURITY

We would also like to draw attention to the next top markets for cyber security as listed below. These markets are not only very large but their governments are increasing their focus and investment in cyber security.

- Malaysia
- South Africa
- Chile
- Poland
- Singapore

CONCLUSION

A New York Times article published in June 2013 (Shanker & Sanger) claimed that the United States, through an unpublicized program, is helping its allies in the Middle East and Asia to build up their cyber security systems. The nations named by the report included the UAE, Saudi Arabia, Bahrain, South Korea, and Japan. Except for Bahrain, which was removed from our list due to the relatively smaller size of its cyber security market, all the other countries are on our list. Thus, our independent research found similar results. According to the report, the Pentagon is currently developing plans to sell cyber security products to these countries and also provide personnel training in those regions. Based on our research, we can conclude that there is significant opportunity in the markets listed in this document and some others, which we hope, will be examined in depth sooner rather than later.

Virginia is an industry hub of cyber security companies. With the increase in cyber-attacks on the private sector and government agencies around the world, there are great opportunities for Virginia's cyber security firms to export their products, services and technology, to governments in the countries mentioned in this report. Defense budgets are being increased to include cybersecurity as cyber-attacks on a daily basis target state-owned energy companies in the Middle East, government agencies in Japan and South Korea or attempt to infiltrate the systems of US agencies. Other nations are also facing these problems. Many large defense firms are already expanding into this cyber area, as it quickly becomes a top priority for many governments around the world.

REFERENCES

AG Reporter (2013) Cyber security awareness increases in the Middle East. *Arabian Gazette*, January 31, 2013. Retrieved on September 20, 2013 from http://arabiangazette.com/cyber-security-awareness-increases-middle-east-20130131/

Al Makaleh, S. (2013). Government, banks bear brunt of UAE cyber attacks. *Gulf News*. Retrieved September 20, 2013 from http://m.gulfnews.com/business/technology/government-banks-bear-brunt-of-uae-cyber-attacks-1.1183442

Boulanin, Vincent. (May 13, 2013). Arms production goes cyber: A challenge for arms control. *Stockholm International Peace Research Institute.* Retrieved from http://www.sipri.org/media/newsletter/essay/Boulanin_May13).

Grauman, B. (2012). Cyber-security: The vexed question of global rules. McAfee/Security and Defense Agenda. Washington D.C.: Geermi Camie.

Hafeez, T. (2011). Symantec launches Norton 2012 plus UAE CyberCrime stats. TBreak Technology. Retrieved September 20, 2013 from http://tbreak.com/tech/2011/09/symantec-launches-norton-2012-plus-uae-cybercrime-stats/

Kallender-Umezu, P. (2013). Japan's new cyber unit understaffed, lacks skills. July 9, 2013. *Defense-News*. Retrieved on September 21, 2013 from http://www.defensenews.com/article/20130709/DEFREG03/307090007/Experts-Japan-s-New-Cyber-Unit-Understaffed-Lacks-Skills

Kolendo, S. (2013). South Korea bolsters cyber security forces. HIS Jane's Defense Weekly, April 4, 2013. Retrieved on September 25, 2013 from http://www.janes.com/article/11782/south-korea-bolsters-cyber-security-forces

Lee, D. Israel tops cyber-readiness poll but China lags behind. BBC News Technology. January 30, 2012. Retrieved on September 19, 2013 from http://www.bbc.co.uk/news/technology-16787509

Market Research, (June 2013). Global Cyber Security Market 2013-2023. London, England: Strategic Defence Intelligence. Accessed on September 18, 2013 via http://www.prweb.com/releases/2013/Cybersecurity-Market/prweb10834320.htm

Miller, J. (2013), Japan's new cybersecurity strategy – Implications for the Alliance. Forbes. Retrieved from http://www.forbes.com/sites/jonathanmiller/2013/06/13/japans-new-cybersecurity-strategy-implications-for-the-alliance/. Accessed on September 19, 2013.

Organization of American States, 2013. Overview of cyber security – Brazil. Retrieved on September 20, 2013 from http://www.oas.org/cyber/presentations/OAS%20set%202012.pdf

Qatar's National ICT Plan 2015. Advancing the Digital Agenda. Retrieved on September 25, 2013 from http://www.ictqatar.qa/sites/default/files/documents/Qatar's_National_ICT_Plan_English.pdf

Shanker, T & Sanger, D. (2013). US helps allies trying to battle Iranian hackers. *The New York Times*, June 8, 2013. Retrieved on September 21, 2013 from

http://www.nytimes.com/2013/06/09/world/middleeast/us-helps-allies-trying-to-battle-iranian-hackers.html?pagewanted=all&_r=1&

Srimoolanathan, B. (2011). Cyber security – From luxury to necessity. Frost and Sullivan. Retrieved from http://www.frost.com/sublib/display-market-insight.do?id=225170420

US Department of Commerce. Commerce Control List, Bureau of Industry and Security. http://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl/

US Department of State. US Munitions List, *Directorate of Defense Trade Controls*, http://www.pmddtc.state.gov/registration/.