The Arab Gulf States
Institute in Washington
Building bridges of understanding

UAE Security Forum:
Bridging the Cybersecurity Talent Gap

Conference Report

The Arab Gulf States Institute in Washington

Building bridges of understanding

May 5, 2016

UAE Security Forum: Bridging the Cybersecurity Talent Gap

Conference Report

Event Report

#2

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.

Photo Credit: ASDA'A Burson-Marsteller

About This Report

This report is based on the discussion that took place during the "UAE Security Forum 2016: Bridging the Cybersecurity Talent Gap" that took place in Abu Dhabi, the United Arab Emirates, on February 21, 2016.

The discussion was captured by Leah Sherwood, Khalifa University of Science, Technology and Research.

The UAE Security Forum 2016 was sponsored by Raytheon Company.

For more information visit www.uaesf.org.

Contents

Welcome Letter

Ambassador Marcelle M. Wahba, AGSIW President

Dear Colleagues,

It gives me great pleasure to present the final report of the UAE Security Forum 2016: Bridging the Cybersecurity Talent Gap.

With the increasing revolution in information technology, cybersecurity joins defense and water, food, and energy security as a core national security imperative. On February 21, the Arab Gulf States Institute in Washington and Raytheon Corporation brought together cybersecurity experts, government officials, educators, and employers for the inaugural UAE Security Forum in Abu Dhabi. The goal of the forum was to explore ways to help bridge the gap in cyber curriculum and cyber training programs through dialogue with major academic institutions, government officials, and industry leaders.

Given the ever-intensifying digitization of modern societies, and the enormous quantity of sensitive personal, corporate, and national information transmitted around the world at any given moment, serious cybersecurity measures are essential to protect critical national infrastructure and sensitive public and private sector data. Without vigilant cybersecurity measures, critical information is potentially vulnerable to online criminals, identity thieves, malicious hackers of all kinds, state-sponsored cyber economic espionage, and the growing specter of cyber terrorism.

The need to develop cyber talent and expertise in Gulf Cooperation Council countries has never been more urgent. The United Arab Emirates has taken a key leadership role by preparing young Emiratis to perform competitively at a world-class level in the technological fields and disciplines central to our rapidly developing economy and information era.

The recently adopted UAE science, technology, and innovation higher policy is a good example of the kind of government initiative necessary to develop the capabilities and workforce capacity needed to meet these challenges, particularly by intensifying its focus on STEM (science, technology, engineering, and math) education and innovation. However, even with such enlightened policies, the reality is that cyber talent is in high demand, difficult to develop, hard to identify, and even more difficult to recruit. To develop the requisite workforce for this future, new systems and technologies will be required to ensure that the processes of recruiting, training, and retaining workers are all done successfully. It is essential that cybersecurity comes to be recognized as a career path in its own right.

The UAE Security Forum, under the title "Bridging the Cybersecurity Talent Gap," sought to explore best practices and make recommendations about how to tackle these challenges by bringing together government officials, educators, and industry executives in a number of interactive sessions during the day-long event. This report, summarizing the discussion and recommendations, is aimed to help enhance cybersecurity by building capacity across the board, and in particular contributing to the development of an Emirati workforce that can meet urgent challenges.

I would like to thank our partners, Khalifa University of Science, Technology and Research, as well as The National newspaper, AmCham Abu Dhabi, and the U.S.-U.A.E. Business Council. Above all, I would like to thank our sponsor Raytheon, without which this forum would not have been possible. I hope you find this report informative and useful and look forward to the next iteration of the UAE Security Forum in 2017.

Sincerely,

Ambassador Marcelle M. Wahba
President, Arab Gulf States Institute in Washington

Executive Summary

The Middle East experiences a particularly high level of cyber threats and attacks, primarily because of the number of valuable targets and pervasiveness of technology. In the Gulf Arab states, cyberattacks targeting key installations cost an estimated $1 billion annually. Due to the intensity and extent of cyberattacks, the United Arab Emirates has committed a significant portion of its economic development plan to cyber capability. Indeed, a digitalized national development agenda promises continued innovation, productivity, and economic growth, but it also necessitates a successful navigation of the evolving cyber threat environment and its associated ecosystems. Therefore, it is essential that the UAE build upon progress already made and provide the resources needed for continuous development in cyber capability and the mechanisms that support cyber resilience.

In the cyber realm, there is no end point upon which cyber security is assured. It is a continual process of development and reform. The UAE Security Forum highlighted what has been done in the cyber field and what still needs to be accomplished. In the UAE, the groundwork has been laid to create a platform upon which national cyber capability can grow. A significant part of the foundation was the development and dissemination of a national cyber security strategy in 2012 coupled with the establishment of relevant legal instruments needed to enforce compliance and standards. The provision of political and financial support to Khalifa University to establish the Information Security Centre to prepare Emirati youth for careers in the cyber field is a good illustration of preparatory efforts. Government initiatives to inspire interest in the cyber field and increase awareness about cyber threats have also proven to be productive. Knowledge of cyber threats is key to countering the risks that accompany the Internet of Things, which is being woven into the fabric of the UAE's society.

In the cyber realm, there is no end point upon which cyber security is assured. It is a continual process of development and reform. The UAE Security Forum highlighted what has been done in the cyber field and what still needs to be accomplished.

Alongside these advances there remain precarious gaps. More needs to be done to boost the UAE's cyber capability and bridging the talent gap is a key challenge. The small size of the population places limits on the talent pool and the field is so new that planners in the educational sector have not had enough time to adapt to the burgeoning need in the private and public sector. In this light, it is critical for industry leaders to collaborate with educational institutions to build programs tailored to meet the growing needs. Innovation, critical thinking, and problem solving skills are the hallmark of effective cyber professionals and educational reform is needed to create graduates with strength in these areas. The cyber field needs more than technically oriented workers; it needs an ecosystem that fosters cyber awareness and cyber education. Indeed, collaboration is the key in the next steps toward improving the cyber workforce. Outside the educational sphere, current levels of cooperation and collaboration between agencies are inadequate; vertical and horizontal knowledge sharing across sectors and the public/private divide is a fundamental part of the next generation of cyber defense. Furthermore, preferences for convenience need to be seen as secondary to security. Data

optimization and new technology must be contextualized against the risks they present and soberly weighed.

Ultimately, the cyber community must become more strategic and visionary. Due to the rapid pace of change and the extent of vulnerability, many organizations are inclined to react while only paying lip service to proactive strategies. Planned solutions and strategies pivot around people. Attracting the talent needed for a dynamic cyber force comprised of personnel with technical and nontechnical skill requires that the field offer clear career paths, opportunity for promotion, and specific job titles. Establishing a common nonspecialist language of communication about the cyber realm coupled with short, effective cyber education courses for managers are valuable tools to build cyber capability. There is indeed a lot to be done, but the good news is that the work has already started.

Recommendations

Overarching

- Cybersecurity is a continual process of development and reform. There is no single solution, but a shift of focus from just protection and compliance is critical.
- Capabilities have to be numerous, diversified, long-term, short-term, technical, and nontechnical.
- It is crucial to align around verticals (training, education, and awareness) and integrate them horizontally across sectors and the public/private divide.
- There is a need for more focused cyber academies, cyber innovation centers, and test ranges for testings and simulations.
- Trust must be fostered between the public and private sectors to share information and collaborate by infusing a shared sense of responsibility to defend against cyber threats.
- Proactive and well-planned cyber security solutions depend on people; humans, not technology, are the key. The real problems, and solutions, start with them.
- Individuals who combine soft skills and some technical cyber skills are integral parts of any team. Social science scholars, public servants, diplomats, and policy practitioners are all needed in the cyber sphere.
- It's crucial to identify real problems, not abstractions and demand secure technology as part of new product designs.

Education

- The talent gap has arisen mainly because of misperceptions about the field and unclear career paths, due to the nature of cybersecurity as a new area of study.
- Schools should provide more cyber relevant activities and cyber career information.
- It is critical for industry leaders to collaborate with educational institutions to build programs tailored to meet the growing need to infuse innovative thinking in students with technical skills, but who also strive to continuously learn and who excel at problem solving.
- Cyber fundamentals must be integrated into other educational disciplines, especially the STEM fields. The goal is to promote a mindset that combines technical competency with social and critical thinking skills.
- Readily available test and simulation envirmonments will help hone cyber skills and develop an effective workforce.
- Government education initiatives to promote interest in the cyber field and increase awareness about cyber threats are important.
- Cyber education should start at an early age, not only to create future cyber professionals, but also to generate a population that is cyber aware. Early education can lead to engrained cyber safe practices in daily life, which minimizes threats emerging from the Internet of Things.

Management Should

- Integrate cybersecurity into general risk management approaches aimed at all staff, and invest in continuing education for all senior management and board members.
- Establish a common nonspecialist language for communication on cyber issues, coupled with short, effective cyber education courses for managers.
- Develop new tools for data protection, make better use of existing solutions, and share responsibility and accountability.
- Not be afraid to engage with independent technical communities like hackers, data scientists, and other experts who are often left out of vital conversations.
- Take responsibility for cyber defense. Cyber defense is a shared responsibility across the organization. Mangers must support technologists, not the reverse.
- Accept that while policy leadership is needed, it cannot come from IT departments. Leadership teams have to know the cyber side of the business.
- Develop proper security strategies to prioritize data and critical capabilities, patches and updates, and segment data.
- Establish clear lines of accountability and well-developed disaster recovery plans within and across sectors.

- Adopt a risk-based approach and know what indicators reflect success.
- Invest in and encourage continuous cyber security training and education.

Awareness and Recruitment Should

- Create a modern taxonomy of the cybersecurity profession based on interagency efforts. Clear job titles, growth ladders, and explicit job descriptions are essential.
- Recognize that millennials are a key source for cyber recruitment and require more interaction with cyber professionals; mentoring programs are excellent engagement tools.
- Prioritize informing women about careers in cybersecurity as they are a key target for recruitment for future cyber defense forces.
- Move past outdated human resource models of hiring toward an appreciation of new factors such as nontraditional career paths.
- Develop “tiger teams” to improve workplace retention and focus on learning and talent development to ensure the quality and quantity of the labor force that will be required in the future.
- Invest in cyber day and residential camps as recruitment, training, and awareness tools.

Introduction

The Arab Gulf States Institute in Washington partnered with Raytheon and Khalifa University to host the UAE Security Forum in Abu Dhabi on February 21. It was a rare cyber event bringing together technical and nontechnical constituencies. The event offered perspectives from government, academia, and industry that ranged from the conceptual and holistic to the technical and practical. Perhaps the spectrum of viewpoints delivered in plain language was the greatest contribution that the forum made as it allowed those familiar with the cyber field to mingle with those just starting to learn to manage it. Connections were fostered between the cyber core and periphery where practice takes place.

The forum began by noting broad agreement that the cyber challenge is mounting, and focused on some of the more pressing challenges. Innovations by cyber criminals have made their activities more pernicious and effective. They are not only exploiting the vulnerabilities inherent to integrated systems, but are ever more successful at gaining access to the intersections of optimized data, which makes their intrusions more dangerous. Another serious problem is the lack of clarity in the minds of public and private sector managers and operators who are told to collaborate, but who have no idea what, precisely, to do. This confusion has sometimes led to inaction and error. The calls for vertical and horizontal collaboration are widespread, but clarity is needed regarding effective means and mechanisms. The management of cyber risk must also shift from cyber technologists to the managers and operators of firms and departments who need to accept this responsibility. That will require the training of managers and executives in cyber fundamentals, and the development of a cyber action taxonomy that is accessible to the nonspecialist and can allow for conversations about cyber security with a broad range of stakeholders. These managers and executives need to understand the cyber components and requirements of their own businesses and communicate them to other parts of their organizations such as human resource departments. Another main challenge addressed by the forum was the problem with cyber talent recruitment – there is simply not enough talent developed at the moment to meet current needs, let alone those of the future.

The event offered perspectives from government, academia, and industry that ranged from the conceptual and holistic to the technical and practical.

The cyber picture is not all negative, of course, and many initiatives, such as cyber camps, are proving to be excellent recruitment, training, and awareness tools. Industry leaders are starting to reach out to schools and universities. Partnerships between agencies and those that bridge the public/private sector divide are thriving. Conversations are starting to acknowledge that leaders are unsure of what to do; that is the best place for constructive discourse to begin as it will lead to engagement, cooperation, collaboration, and new ways of managing. Moreover, national cyber strategies are being developed and continuously updated, while laws are being established to ensure their implementation. The limits of technology are being recognized, but so are important new opportunities such as the role of Artificial Intelligence (AI) in future cyber hunting endeavors. The development of AI will somewhat mitigate the pressure to recruit so much talent, but not alleviate it. Therefore educational programs are increasingly targeting women and children at an early age, both of which are underutilized

resources for this field. Cyber diplomacy is gaining momentum and offering a constructive way to engage for peace and security, although cyber capabilities are a double-edged sword given that in many cases they can also be weaponized.

While a great deal has been done in the cyber field, the road ahead is long. With targeted investment in the right areas, paired with effective collaboration and trust building, the cyber community appears capable of meeting the challenges that lie ahead in the rapidly changing cyber environment. Investing in people is the key solution.

The State of Cybersecurity in the UAE

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 counteract risks. Information is a strategic commodity in today's globalized economy, within which cyberspace is a core dependency. The challenge for the United Arab Emirates is that the volume and speed of dangerous incursions to the accessibility, integrity, and resilience of its critical networked systems and infrastructures are real and mounting. Threats stem from data infringements, criminal activity, and service disruptions. The UAE's principle cybersecurity challenge is rooted in its broader context as a country defined by the Internet of Things. Therefore, the necessity of and reliance on cyber capability underwrites much of the UAE's national security architecture.

Threats to the UAE's networked defense sector infrastructure are significant and on the rise. To offset this 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). From a strategic standpoint, cyber capability, cyber defense, cyber doctrine, and cyber diplomacy all have growing implications for the UAE's virtual threat environment. The reliance on cyber capabilities in energy, finance, aviation, tourism, and governmental service sectors also presents unique challenges. Cyber insecurity in these realms is, in effect, a tax on the UAE's economic growth. Indeed, the same features of its economy that make it a success also expose the country to such risks. Government online portals are being attacked more frequently as they are developed and expanded.

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 counteract risks.

Perceptions about cyber security are another main challenge. Generally, UAE cyber practitioners downplay the role of internal cyber threats, which are the biggest source of insecurity. Aruba Networks revealed that the workforce of UAE's GenMobile, which integrates mobile devices into daily life, are "far more willing [than they ought to be] to share company data, and are notably oblivious towards security." GenMobile employees will continue to represent a key component of the UAE's national workforce and their behaviors require correction. The strategy will require a human-to-human approach rather than one that is device focused. Integrating cybersecurity into general risk management approaches aimed at all staff, as well as investing in continuing education for all senior management and board members, is another identifiable way forward. The primary challenge is to bridge the talent gap and create a future "cyber defense force."

The UAE needs more human capital for its cyber defense force, but it faces a range of predicaments in recruitment, hiring, and training in the cyber sector. Raytheon and the National Cyber Security Alliance's (NCSA) survey on cyber career interest and educational preparedness of millennials aged 18 to 26 produced several important findings: Schools are not providing cyber relevant activities or enough cyber career information or the the skills millennials want to develop, which are the 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.

The UAE needs more human capital for its cyber defense force, but it faces a range of predicaments in recruitment, hiring, and training in the cyber sector.

The UAE has a multipronged cyber strategy. On one hand, it is expected to double its cyber security budget to $10 billion within the next decade. One-third of UAE firms reported cyber security breaches in 2015, and among them just 50 percent had cyber attack contingency measures in place. Only half of the firms hacked were even aware of it. This has led to more investment in awareness campaigns and on educational initiatives particularly for mobile users, who are often easy targets for cyber criminals, as well as for the general public.

NESA published a national cyber strategy with accompanying policies and standards in June 2014. The National Cyber Security Strategy (NCSS) includes the Critical Information Infrastructure Policy (CIIP) and the UAE Information Assurance (IA) standard. Together they form the heart of the UAE's national cyber security and ICT infrastructure approach. Compliance is obligatory. Longer-term initiatives include the development of Khalifa University's Information Security Research Center (ISRC), which offers MSc and PhD degrees in cybersecurity. The center focuses on innovative techniques, protocols, and systems to identify cyber security threats, assess risks, and protect infrastructures while boosting general capability. Complementing the long-term educational and cyber strategies, the UAE government has also established important new legislation on cyber crimes.

The UAE has shifted from a reactive to proactive operating mode on cybersecurity. The UAE's performance reflects an overall balance that includes some successful initiatives with demonstrable and quantifiable results, but there is a great deal left to be done to consolidate what has been achieved and facilitate additional progress. Cyber threats emerge and evolve so quickly that all governments around the world are scrambling to keep pace with these developments and institutionalize frameworks and protocols to meet the threats. In the UAE, the principle challenge lies in in ensuring that all relevant facets of society meaningfully implement new standards versus a pro forma, tick-the-box compliance that cannot be effective.

The UAE's general cyber threat landscape has evolved from lone hackers to sophisticated "cyber brigades" attempting to disrupt the security of the state. The country has committed significant resources to improving its cyber defenses and developing its technical cyber capability. [1]

1 The above references the AGSIW report "Bridging the Cybsersecurity Talent Gap" available at http://www.agsiw.org/uaesf-2016-bridging-the-cybersecurity-talent-gap/.

Resilence and Cybersecurity: How Prepared Are You?

The first panel of the forum, which was moderated by Sharief Fahmy, CEO of Middle East General Enterprises, included Eman Al Awadhi, manager of security compliance operations at du, Michael Daly, chief technology officer of Raytheon Cybersecurity, Ernesto Damiani, director of the Information Security Research Center and professor at Khalifa University, and Paul Rogers, general manager of industrial cybersecurity at GE. The panel focused on real-world cyber experiences and cyber resilience strategies. The panelists agreed that the threat environment for individuals as well as the public and private sectors is increasingly complex and dangerous. For individuals, the Internet of Things (IoT) is both an identity and a security threat because it is integrated into homes, vehicles, and other facets of everyday life, including health records at hospitals and services like wireless electricity. Personal devices, which are often purchased for reasons other than their security features, are rarely patched or updated and are therefore particularly vulnerable. The IoT threat is particularly severe in societies such as that of the UAE where criminals have many opportunities to access sensitive data belonging to individuals. Attacks and other malicious activities aimed at the private sector and governments are also on the rise in such societies. But, awareness of the threat is increasing, with approximately 80 percent of private companies expecting to be attacked. The vulnerability is even greater in the public sector, with 90 percent of critical oil and gas utilities having been attacked, and an overall rate of 70 percent of public institutions being subject to some kind of attack over the past 12 months. The panelists noted that the cyber threat environment has changed from individual attacks launched by lone actors to more permanent, pervasive, and sophisticated threats. Therefore security approaches that emphasize a defensive approach are now outmoded, and proactive strategy has become a requirement.

The vulnerability is even greater in the public sector, with 90 percent of critical oil and gas utilities having been attacked, and an overall rate of 70 percent of public institutions being subject to some kind of attack over the past 12 months.

The interconnectivity of infrastructure has further modified the nature of threats. Physical critical infrastructure and cyber capabilities are now shared on a local and global scale, but risk analysis and evaluation is not uniform and cyber defense is typically poorly integrated. This exacerbates vulnerability because compromises to one system affect many others. The attack against the U.S. department store Target through its air conditioning system is a classic example of this new kind of interconnected threat. To counter such attacks, cyber defenses need to incorporate new levels of interconnection, both vertically (from the bottom to the top of the organization's hierarchy) within given structures, and horizontally (between partnering organizations, their managers, and so forth). Increasingly connecting data for convenience is another new trend that leaves systems susceptible to attack. Data optimization creates more intersections where valuable data can be taken. Connecting the core with the periphery in any system is risky, and cyber criminals have benefited from this pattern. They have also begun collecting data that corresponds to structures of decision making. Industrial control systems are increasingly online, and the depth of penetration of this environment is another evolving threat. These controls can be disrupted by disabling emergency response systems or even

supply chains. Eighty percent of global cyberattacks are from this kind of "spear phishing."

Moreover, there is a shortage of qualified personnel to meet these challenges and defend against cyberattacks. The lack of sufficient cyber talent is a considerable gap in cyber defense, and private companies often outbid governments to recruit the best talent, leaving the public sector with insufficient qualified manpower. The new generation of "Millennials" represents a key area of recruitment potential and a survey conducted by Raytheon and the NCSA showed some strategic areas for investment to recruit more young talent. One finding was the need to communicate the message that cyber careers are not entirely technical and screen oriented, which will make this profession more attractive to millennials who seek engaging jobs. Interacting with cyber professionals, learning about the cyber field at a very young age, and involving women were also clear areas of potential improvement. However, hiring cyber talent involves more than just recruiting personnel who are qualified as Certified Information Systems Security Professionals (CISSP), although there is a need for staff that has such technical skills.

The lack of sufficient cyber talent is a considerable gap in cyber defense, and private companies often outbid governments to recruit the best talent, leaving the public sector with insufficient qualified manpower.

Recruiters are seeking dynamic people such as those with a deep understanding of the industry they serve, who recognize the precise cyber capabilities of that space in terms of scope and protocol and have the experience to credibly manage it. Meeting cyber recruitment needs is challenging human resource departments to move past outdated models of hiring that are excessively based on education and formulaic experience models toward a greater appreciation of new factors. The panelists offered examples of how the best new cyber talent now often comes from people without academic degrees or formal cyber work experience. Human resource-specific solutions center on new hiring protocols as well as new means of retaining talent after what is usually a heavy training investment made in them. Even with cutting-edge hiring practices that may shrink the gap, the panelists predicted that the future of cyber defense will not be based on a force of low-level technical warriors; the frontline defense will instead be provided by Artificial Intelligence (AI), with humans filling jobs requiring more sophisticated judgment.

Solutions to the myriad of cyber challenges rest in large part with educational institutions, which will increasingly work in partnership with industry to customize programs to meet future demands. There is a need for high quality computer scientists with expertise in cyber relevant areas. However, the technologists cannot meet the cyber challenge by themselves. There is also a growing demand for more rounded individuals with some technical cyber skills, matched by softer skills and social science backgrounds. This will allow for critically-important bridging of technical and nontechnical aspects of the cyber field. One way to promote this is to advertise cyber careers to social scientists and provide on-the-job training for them. The development of new tools for data protection, the better use of existing solutions, and an emphasis on shared responsibility and accountability should all continue to be developed. One promising idea is to take advantage of expertise in independent technical communities like hackers, data scientists, and other experts who are often left out of political conversations. Cyber literacy challenges are also an excellent means of engaging the community, particularly

youth, and training employees of all types. Training and learning are essential components of broader cyber strategies, particularly given that the field will continue to change rapidly.

The State of Cybersecurity: Where Are We in 2015?

John C. Inglis from the Venture Partner Paladin Capital Group and the former deputy director of the U.S. National Security Agency discussed "The State of Cybersecurity: Where are we in 2015?" The central theme of his presentation was that many cyber professionals are focusing on what he called "first order phenomena" and therefore fundamentally misread the strategic domain. For example, the cyber realm is often viewed horizontally, while in fact it is really a vertical overlay of technology, people, and process. Cyber practitioners, according to Inglis, try to fix the wrong things and hold the wrong people accountable. Inglis stressed the multidimensionality of cyber challenges and solutions. He criticized flat assessments and approaches on the grounds that any cyber solution must include all three of those components. Most cyber problems and their solutions are not technology-based, he said.

Inglis asserted that we defend the wrong things when we concentrate primarily on operating systems, remedies to links, or patching, because these are all mere abstractions and are neither the data itself nor the supporting infrastructure. When the focus is transactional or tactical, it is incorrect. He emphasized the need to stop looking at quantitative transactions at the periphery and worrying about averting a cataclysmic event. He urged professionals to pay more attention to the "slow rot" already setting into the systems, which is far more threatening than external menaces. Cyber security efforts also defend the wrong time, Inglis continued. It is an unsound strategy to embrace new technology and fix it retrospectively because that is accepting collective vulnerability and then striving for collective defense. Technology should only be used after it is made safe. In referring to "the wrong people," he means that technologists should not be held accountable for cyber defense. They are not the ones who calculate risk and cost. Managers must be responsible and determine the right balance of inputs. Mangers must support technologists, not the reverse. This requires managers to be better trained in cyber concepts and become conversant in a nonspecialist language to communicate technical issues. This will help tip the balance away from the overemphasis on technologists who are ill-suited to the task.

The cyber realm is often viewed horizontally, while in fact it is really a vertical overlay of technology, people, and process.

Adding to the list of poor practices, the security strategies of government agencies and private companies too often boil down to little more than presentations based on tactics that are incoherent because they are the sum of what has been learned based on past experience. This is not the architecture of a proper security strategy. Everyone has a responsibility for security within as well as across departments and agencies. Currently, the private and public sectors are confused about their roles and how to complement one another without compromising themselves. This arises because of a lack of clarity regarding who should do what, coupled with misunderstandings of the critically important difference between cooperating and collaborating. Collaboration is not the division of labor; it is the sharing of concerns, discussion of institutional and management challenges, trust, and professional intimacy. To collaborate

is to offer help, not to divide work or agree to coexist.

Sound security strategies prioritize data and critical capabilities, ruthlessly patch and apply updates, and segment data and critical capabilities, in addition to proactively targeting specific locations. They also include sharing details and establishing clear lines of accountability for cyber defense within organizations and departments, and within and across sectors. Lastly, they must Include a well-developed disaster recovery plan. This helps managers know where to make strategic investments in advance, in order to minimize the worst-case scenarios. Inglis cautioned against action without factoring in people and treating the problem as horizontal. It is key to invest energy and resources to: create proper security strategy architectures, define institutional collaboration in practical terms, and enable engagement with managers by building bridges between technical and nontechnical employees. Furthermore, he strongly advised institutionalizing the practice of identifying real problems, not abstractions, and demanding secure technology as part of new product design.

Central to overcoming cyber insecurity is to transcend what Inglis called "the engineer's mind," a mentality that is not trained to see, let alone address, wider issues. Engineers think in terms of physical systems, security, networking, data structure, and programming. This narrow scope gives cyber adversaries an advantage since they take into consideration policy, law, ethics, social behavior, and human psychology, as well as programing. People are the weak link in cyber space, and both real problems and solutions start with them. The realm of the cyber environment is far bigger than just computer science. Systems thinkers, social scientists, civil servants, diplomats, and policy practitioners must all develop a working familiarity with cyber space. There is a minimal level of cyber literacy that everyone now needs and, therefore, the demand for nontechnical knowledge and training workshops will only grow.

Cyber diplomacy is already part of international relations, adding another dimension to cyber strategy. Indeed, cyber space has ushered in a new geography that can either stimulate or inflame geopolitical circumstances.

Cyber diplomacy is already part of international relations, adding another dimension to cyber strategy. Indeed, cyber space has ushered in a new geography that can either stimulate or inflame geopolitical circumstances. Cyber space is also increasingly used to resolve disputes and conflicts that used to be dealt with in physical space. An example is North Korea's attack on Sony ahead of the release of the movie "The Interview," about an assassination attempt on the country's leader, Kim Jong-un. Pyongyang's rationale was that it had been disrespected and had to retaliate. Indeed, cyber space has created a forum for people to organize along ideological lines independent of geography, form mass movements, and mobilize based on shared beliefs (positive or negative). While it provides a new landscape for popular mobilization, Inglis suggested cyber space will not transform fundamental social realities. The disparity between rich and poor, the need for more tolerance and respect, and tensions over religion and politics are enduring human dynamics, but they are now played out in cyber space as well as more traditional terrains.

Creating a 21st Century Cyber Force

The overarching recommendation produced by the workshop, "Creating a 21st Century Cyber Workforce" – moderated by Lydia Kostopoulos, an assistant professor at Khalifa University – was for more capability building. There are various ways to build capability, and recognizing the existing and potential platforms for developing capabilities is the first step in expanding them. On a strategic level, the cyber realm has become a new theater of warfare, which is no longer limited to air, land, and sea. The cyber dimension can be used as either a weapon of conflict, or a tool for peace and diplomacy. Decisions about whether to seek reconciliation or retaliation have been elevated to a strategic level. On a practical level, it is not enough for capabilities to simply be numerous, they must also be diversified. In order to achieve this, long-term, short-term, technical, and nontechnical capability development is required. Adopting risk-based approaches and identifying the indicators that most accurately reflect success or failure will help counteract threats created by the relentless expansion of cloud technology, the IoT, and cyber-related developments such as "smart city" applications.

The workshop focused on the role of education and educational institutions. Education is indeed the solution to the talent gap, and the right education can produce more dynamically skilled, innovative graduates who have technical skills, but also excel at problem solving and strive to continuously learn. Complex problem solving is the number one quality in demand according to the World Economic Forum. Innovative thinking can be taught and it is a critically important skill in the cyber field, particularly since cyberattackers are highly adaptive, innovative actors, who must be matched by defenders. New educational programs and courses can also serve as bridges between the cyber field and other sectors. Cyber skills must also be integrated into other educational fields, especially the Science, Technology, Engineering, and Math or STEM fields. A technical worker who also has social and critical thinking skills will become an increasingly prized asset.

Education is indeed the solution to the talent gap, and the right education can produce more dynamically skilled, innovative graduates who have technical skills, but also excel at problem solving and strive to continuously learn.

In general, the private sector must become better at engaging academics and cooperating with governments to create long-term strategies to promote mindsets that understand cyber realities but also think critically. Ultimately, effective and continuous training after graduation is the key to aligning the vertical features of the cyber ecosystem. Twenty percent of the world's jobs are projected to be related to AI by 2020. Future recruitment will become more specialized because AI will increasingly serve the basic functions now performed by many human workers. Partnerships are the wave of the future. Universities, in collaboration with industry, are well suited to run hackathons, competitions, brain camps, and awareness campaigns, for instance. Such activities serve as an ideal trio of capacity building, awareness spreading, and security enabling. Competitions are also helpful in recruiting students and provide a way to expose youth to different areas of the cyber universe, dispelling myths about careers in this field. Importantly, they offer students a chance to see what a job looks like in practical terms and give students the right motivation and an attainable goal. Today, most competitions mainly attract boys. Efforts must be made to attract female students and inform them about what these careers offer. Notably, the number of young women video gamers has

surpassed that of young men. Young women offer great promise as future talent.

The workshop participants recommended that cyber education start at a very early age, not only to create future cyber professionals, but also to foster a population that is cyber aware. Early education on cyber best practices can lead to engrained cyber safe practices in daily life, which minimizes the threat of the IoT. The participants agreed that children must be taught about cyber risks, starting as early as elementary school – but equally important, they must not be frightened by the information. Cyber camps, day camps and residential camps for older children were recommended based on their established records of success. Camps have gotten students excited about cyber topics and have proved to be an effective venue for them to talk to older youths about how to continue their education. Camps can map out career paths and make them exciting. A variety of camps exist already, with some aimed at educating teachers on how to incorporate cyber topics into their curricula (until standalone courses are approved), while others expand existing skillsets or teach new ones. Advanced camps should be created to build upon what has been established. In terms of numbers, the most successful camps are those that offer team-oriented exercises, having the added benefit of developing "soft" and social skills. Posters, games, and prizes are solid ways of drawing attention to cyber field career options, and cyber competitions can provide platforms for mentorship. People will get excited if they understand how much these subjects can matter to them personally.

Public, private, and education sector collaborations must involve human resource specialists. These specialists need new information on emerging requirements and trends, and need training in order to create effective new human capital recruitment plans. HR managers should make a practice of routinely conducting new workforce data analyses. The creation of a modern taxonomy for the cyber security profession, which is based on interagency dynamics, was a key suggestion. This will help create the requisite job titles and descriptions that inform employers and employees. Generic job titles such as "Informational Specialist" lack clarity and allure. To attract talent, the cyber field needs to be "professionalized" and clear career paths established to retain the employees who are hired. The opportunities for promotion and progressive career development has to be explicit. Outmoded pedantic and prescriptive HR departments must become more flexible and find new ways of perceiving potential in people.

To attract talent, the cyber field needs to be "professionalized" and clear career paths established to retain the employees who are hired.

Organizations can also help solve some of the practical challenges around recruitment and retention. On one hand, those who know what is needed can feed that information to HR rather than waiting for the department to provide what it believes the organization is seeking. Therefore, active participation in the establishment of an HR cyber security framework is a good way to code jobs as well as insert key words and use them in many capacities, including job advertisements. On the other hand, the participants recommended the creation of "tiger teams" that work on retention in the workplace, and focus on learning and talent development to create the required labor volume. They can find niches in the educational system and work informally as cyber coaches or leaders in exercises such as "cyber jams." The private sector can also collaborate to establish a cyber reserve force that is external to individual organizations, but is on call in case of a crisis. This reserve force can be comprised of people who work elsewhere, but are reassigned until the problem is solved. A participant recommended some

firms build their own educational institutions or design courses to train recruits and start to generate their own workforce, as applied by Ratheon Foreground Security. This is also a potential venue for running controlled hacking experiments to help design strategies to counter cyberattacks and customize responses that avoid falling into a one-size-fits-all pattern.

Metrics are a big part of the cyber field, including delivery metrics, human metrics, and work metrics (how much time to find, isolate, and eradicate the threat). However, the most significant progress needs to be made with the managers and leaders of departments and organizations. Beyond understanding their own businesses, they need more awareness of the workflow within them in order to understand the potential cyber risks they face. It is no longer possible to rely on the IT department to keep the company safe. Policy leadership is needed and that cannot come from the IT department. Leadership teams have to know how the cyber side of the business actually works. Leaders and managers should be familiar with their cyber security posture as well as what standards are used and how they are met. People, not technology, are the solution to cyber threats. David Amsler of Raytheon Foreground Securities noted that in 2015, all major sophisticated attacks on his customers were detected by humans, not technology. Ironically, people are also the root cause of the problem, so part of the solution is to improve the capability of people to reduce human error and mitigate problems caused by poor hardware. In short, there is a need to align around the verticals of the system like training, education, and awareness and then integrate them horizontally to produce powerful tools for managing the new cyber ecosystem. Ultimately, it is important to recognize that this task will never be completed. Cybersecurity does not have a point solution; it is a continual process.

Agenda

February 21, 2016

Welcome Session:

Remarks By:

Christopher Davis, Country Leader/President, Raytheon International, United Arab Emirates

Ambassador Marcelle M. Wahba, President, Arab Gulf States Institute in Washington

Opening Keynote:

Tod A. Laursen, President, Khalifa University of Science, Technology and Research

Session 1: Resilience & Cybersecurity: How Prepared Are You?

Moderator:

Sharief Fahmy, CEO, Middle East General Enterprises

Speakers:

Eman Al Awadhi, Manager, Security Compliance Operations, du

Michael Daly, Chief Technology Officer, Raytheon Cybersecurity

Ernesto Damiani, Professor and Director, Information Security Research Center, Khalifa University of Science, Technology and Research

Paul Rogers, General Manager of Industrial Cybersecurity, GEvisit site

Keynote: The State of Cybersecurity: Where Are We in 2015?

Introduction By:

Christopher Davis, Country Leader/President, Raytheon International, United Arab Emirates

Remarks By:

John C. (Chris) Inglis, Venture Partner Paladin Capital Group, Former Deputy Director, U.S. National Security Agency

Session 3: Creating a 21st Century Cyber Force

Moderator:

Lydia Kostopoulos, Assistant Professor, Institute of International and Civil Security, Khalifa University

Speakers:

Fadi Aloul, Professor of Computer Science & Engineering, Director of the HP Institute, the American University of Sharjah (AUS), UAE

Nourah Al Suwaidi, National Cybersecurity Capability-Building Program Manager, National Electronic Security Authority (NESA), the UAE

David Amsler, President & CIO, Raytheon Foreground Security

Steven Hawkins, Vice President, Intelligence, Information and Services, Raytheon

Diane Murphy, Chair, Information Technology and Management Science Department, Marymount University

Michail Maniatakos, Assistant Professor of Electrical and Computer Engineering, New York University-Abu Dhabi

Victor Piotrowski, Lead Program Director, National Science Foundation

Jean-Marc Rickli, Assistant Professor, Department of Defence Studies; Senior Researcher, Near East Center for Security and Strategy, King's College London

Dwayne Williams, Associate Director, Technology and Research; Director, National Collegiate Cyber Defense Competition, Center for Information Assurance and Security at The University of Texas at San Antonio

Session 4: Recommendations and Next Steps

Moderator:

Ambassador Marcelle M. Wahba, President, Arab Gulf States Institute in Washington

Speakers:

Christopher Davis, Country Leader/ President, Raytheon International, United Arab Emirates

Sharief Fahmy, CEO, Middle East General Enterprises

Lydia Kostopoulos, Assistant Professor, Institute of International and Civil Security, Khalifa University of Science, Technology and Research

UAESF 2016 Highlights

"The UAE Security Forum provided a unique and valuable platform for interactive dialogue between cybersecurity experts from the United States and the United Arab Emirates. I was impressed with the cyber maturity and commitment of our partners and look forward to sustained dialogue and engagement." ***John C. (Chris) Inglis, Former Deputy Director and Senior Civilian Leader of the National Security Agency***

"We were grateful for the opportunity to be the academic partners of the UAE Security Forum. The event gave access to our young students to the assembled expertise in the room and inspired them for the opportunity they can have in the future to contribute to this sector." ***Tod A. Laursen, President, Khalifa University of Science, Technology and Research***

"The success of the UAE Security Forum provided the perfect launching point for Raytheon's week of cyber educational engagement in the UAE. The forum was a strong success, bringing together a diverse and talented group of people to focus on cybersecurity and the development of expertise to meet the global security challenges in this crucial domain." ***David C. Wajsgras, president of Raytheon Intelligence, Information and Services***

"The UAE Security Forum was one of the best cybersecurity related events to take place in the UAE. I was happy to take part and delighted that some of my students were able to attend and participate." ***Fadi Aloul, Professor of Computer Science & Engineering; Director of the HP Institute, American University of Sharjah***

"The selected topics at the UAE Security Forum tackled some of the main challenges in the information security field, and the diverse background of the invited speakers led to excellent discussions. I look forward to participating in the next UAE Security Forum." ***Eman Al Awadhi, Manager of Security Compliance Operations, du***

UAESF 2016 Newsfeed

Over 100 cyber security experts gathered in Abu Dhabi on Sunday to talk about the latest challenges of cyber security, during the one day UAE Security Forum, organised by the global technology and cyber security company Raytheon and the Arab Gulf States Institute in Washington. – ***Khaleej Times***

اجتمع أمس أكثر من 100متخصص من القطاع الحكومي و الخاص و الأكاديمي في «منتدى الإمارات للأمن» برعاية شركة «ريثيون» و تنظيم من «معهد دول الخليج العربية في واشنطن» وسط إهتمام كبير في فندق قصر الإماراة في أبو ظبي. – ***Al Bayan***

The conference brought together industry, government and education officials to assess the issue. The institute said cyber-attacks on "key installations" in Arabian Gulf states cost US$1 billion (Dh3.67bn) a year – an amount it expected would increase. In 2014, the UAE had a 400 per cent increase in such attacks, the institute said. – ***The National***

ركز المنتدى خلال عدد من المحاضرات و ورش عمل و الجلسات التفاعلية على قضية محورية على المستوى الدولي و الأمن الإقليمي و الوطني و هي العمل على سد فجوة المواهب السيبرانية. – ***Al Watan***

Speaking at the UAE Security Forum (UAESF) 2016, Dr. Ernesto Damiani, professor and Director of the Information Security Research Center at Khalifa University, said that the UAE is a worldwide leader in the density of its data-collecting sensors per square meter – a move towards efficiency but not without risk. – ***Gulf News***

بدورها، علقت سعادة السفيرة مارسيل وهبة، رئيسة «معهد دول الخليج العربية في واشنطن» على نجاح المنتدى : «لقد إستطعنا تغطية عدد كبير من الموضوعات المهمة خلال يوم واحد، و قد إتخذنا عدد من الخطواط البنائة اليوم.» – ***Alroeya***

Event Sponsor

Raytheon

Raytheon Company is a technology and innovation leader specializing in defense, civil government and cybersecurity markets throughout the world.

Event Partners

KHALIFA UNIVERSITY

Khalifa University of Science, Technology and Research is an independent, non-profit, coeducational institution inaugurated in 2007 as part of an Abu Dhabi Government initiative. Khalifa University is supported by the UAE government and owned entirely by the Emirate of Abu Dhabi.

TheNational

With more than 200 journalists based in the United Arab Emirates and in foreign bureaux throughout the world, The National tells the story of the Middle East as seen through the region's eyes. Focused on the capital, Abu Dhabi, but anchored in the new social and political reality that is the emerging nation within a fast-changing global context, The National offers fresh, compelling content that's made in the UAE.

AMCHAM ABU DHABI
Member of the Global Network of American Chambers of Commerce

Since 1986, AmCham Abu Dhabi has worked to increase trade, investment, and goodwill between the United States of America and the Emirate of Abu Dhabi. AmCham Abu Dhabi is an independent, not-for-profit trade association comprised of Fortune 500 corporations, small and medium sized companies, and prominent business leaders and entrepreneurs.

U.S.-U.A.E. Business Council
usuaebusiness.org

The U.S.-U.A.E. Business Council is the premier business organization dedicated to advancing bilateral commercial relations. By leveraging its extensive networks in the U.S. and in the region, the U.S.-U.A.E. Business Council provides unparalleled access to senior decision makers in business and government with the aim of deepening bilateral trade and investment.