Cyber Capability in the Middle East

Seizing Opportunity while Managing Risk in the Digital Age

by

Roger Cressey
cressey_roger@bah.com

Mahir Nayfeh
nayfeh_mahir@bah.com

Booz | Allen | Hamilton
delivering results that endure

Cyber Capability in the Middle East

Seizing Opportunity while Managing Risk in the Digital Age

The development of the Internet and revolutionary digital communication technologies have converged to create a cyber environment that has transformed how individuals, businesses, and governments interact. Cyberspace, comprised of networks, computers, software, hardware, and other devices that store and exchange information across the globe, drives the world economy and allows individuals to connect and collaborate across organizational, social, and geographic borders. Countries and organizations that successfully adopt innovative technologies, master new industries, and maximize the value of cyberspace will strengthen their economies, enrich their societies, and emerge as important players on the world stage.

Nations with a robust infrastructure, investment capital, a culture of business innovation, and an educated and skilled populace will gain the most from operating within this unique domain. Gulf Cooperation Council (GCC) states, sitting on a wealth of natural resources and burgeoning investment, are poised to maximize the potential opportunities offered in the digital world. As a region experiencing strong economic development and significant increases in Internet penetration over the last several years, a promising scenario is evolving in which Gulf states embrace advanced cyber capabilities in order to take full advantage of digital opportunities.

However, growing digital enablement brings with it unprecedented cyber vulnerabilities. Sophisticated computer viruses penetrate previously secure boundaries every day, and increasingly complex cyber threats against a broader range of targets are certain to continue. Balancing risk and opportunity in cyberspace presents governments and organizations all over the world with a formidable challenge. In order to reap the benefits of the digital age without compromising vital assets, nations must engage in rigorous efforts to develop integrated strategies to strengthen cyber capabilities while building trusted and secure environments that protect critical infrastructures and intellectual property—striking the optimum balance between seizing opportunity and managing risk.

The Expanding Cyber Landscape in the Middle East

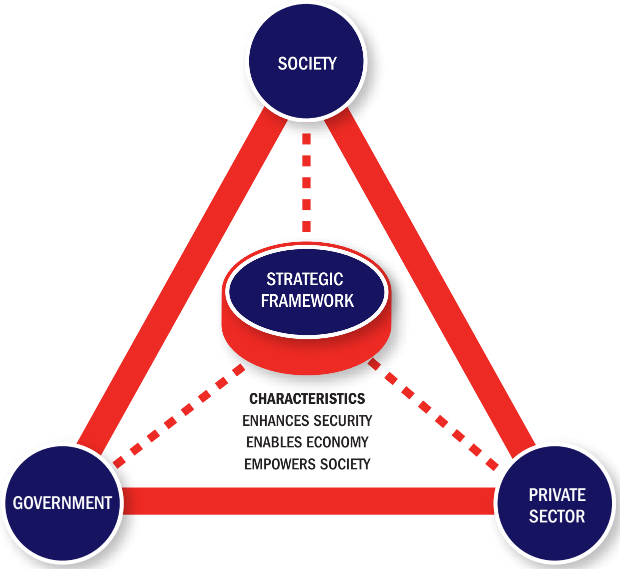
The Middle East has seen significant economic growth in recent years. Infrastructure investments have allowed many states in the region to diversify their economies beyond the energy sector, leading to increased employment levels. This has coincided with the widespread adoption of digital technologies as the GCC states move rapidly into the cyber age. The combination of improved cyber capabilities and tighter integration into the global economy magnifies the growth potential in both established and emerging industries. The convergence of the region's relatively new cyber infrastructure with the maturity of infrastructure investments has many states primed for continued economic and social growth. A wealth of natural resources, rapid economic development, growing populations, accelerated adoption of digital technologies, and increased connectivity are enriching the lives of citizens and make the Gulf an attractive area for global investment. GCC governments are carefully evaluating their strategic capital investments in both physical and digital national infrastructure in order to continue to improve the well-being of states and their citizens.

Economic Diversification and Growth: Every day, foreign exchange transactions worth over $3 trillion are conducted online. Global e-commerce is increasing 13.5 percent per year and expected to top $1.25 trillion annually in 2013. In the energy sector, 300,000 kilometers of electronically controlled lines carry 4 billion gigawatts of power per year. Advanced air traffic control and scheduling systems empower airlines to shuttle more than 700 million passengers across the globe each year.

Noteworthy trends in the Middle East include a more than 300 percent surge in both the number of people accessing the Internet and mobile/cellular subscriptions from 2005 to 2011, according to the United Nations International Telecommunication Union. In addition, the GCC states in particular are integrating cyber technologies into core industry sectors to achieve improved efficiencies and better protect digital control systems and critical infrastructures.

The opportunities offered by cyber technologies make traditional geographic boundaries obsolete in the digital world. Governments must recognize the realities of increased exposure to cyber threats and adopt an appropriate approach for managing cyberspace. Many GCC government and commercial entities are now building or enhancing their existing telecommunications and data infrastructures. They therefore have an opportunity to address cybersecurity and to integrate leading security practices as part of their overall expansion of telecommunications and data services. Doing so will allow the region to consolidate and protect the significant economic achievements of the past decade.

Exhibit 1 | Foundation for a Successful Cyber Infrastructure



Source: Booz Allen Hamilton

As engines of global economic growth that increasingly rely on cyberspace for economic, governmental, and civil activities, Gulf states must recognize the need for strong cyber defense capabilities. They must continue to apply international best practices and security standards in the further strengthening of cyber networks, and they must continue to expand awareness of cyber vulnerabilities through education and public information campaigns. In this way, Gulf states can improve their overall cybersecurity posture and help ensure the long-term viability of their resources.

Developing Integrated Cyber Strategies

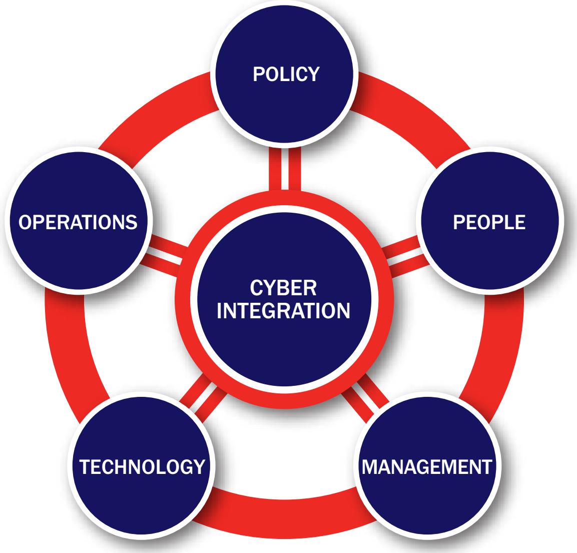
Government, business, and civil society each stand to benefit greatly from a successful and thoughtful cyber strategy, as illustrated in Exhibit 1. Each sector contributes to a sturdy foundation of innovation, economic diversification, long-term growth, and sustained competitive advantage. Government can use cyber capabilities to improve public services and defend critically important assets, both public and private. Many e-government initiatives have already been successfully implemented in GCC states, putting them far ahead of most developed nations in this regard. Businesses across nearly every industry can utilize cyber capabilities to improve products and services, reduce costs, and reach a broader customer base. Civil society and citizenry are enriched by increased access to markets and information, both local and global.

In the highly integrated cyber world, security and stability are in the interest of every stakeholder. Cybersecurity and enablement go hand in hand and should not be viewed as competing interests. If the cyber environment is viewed as a trustworthy and safe place to conduct business, citizens and private organizations are more likely to fully take advantage of increased capabilities, enriching themselves, their companies, and their nations.

The airline industry provides an apt analogy. Safety regulations exist to help prevent crashes and other safety mishaps, and in doing so preserve public confidence in the industry as a whole, to the benefit of both airlines and their customers. Similarly, e-commerce is built on a foundation of faith in secure transactions in cyberspace. If one online merchant breaks that trust, even unwittingly through unsecure operations, the detrimental effect will cascade and hurt other retailers as well by driving customers away from the entire online market. A successful cyber strategy integrates key stakeholders and draws upon shared interests to align efforts aimed at promoting secure and productive activity in cyberspace.

Like other rapidly growing regions that are becoming increasingly integrated into the world economy, the Gulf region must devise a holistic approach to effectively manage its evolving cyber capabilities. The key to growing and securing capabilities in cyberspace is integration. As shown in Exhibit 2, stakeholders must adopt a collaborative approach with clearly articulated goals, objectives, initiatives, and metrics that aligns the efforts of all parties to address five strategic pillars: Policy, People, Operations, Technology, and Management. It is our belief that these pillars—when guided in a coordinated fashion—are the core focus areas for cyber enablement and security.

Exhibit 2 | Five Strategic Pillars of Cyber Integration



Source: Booz Allen Hamilton

Policy

A coherent policy that is created collaboratively is integral to effectively managing resources, reducing unnecessary conflict and redundancy, and working toward long-term goals. Because no single organization owns or controls cyberspace, it is important to maintain a policy that establishes guidance and responsibility, laying out what needs to be done and who has the authority to do it. Policy should be guided by the goal of establishing trust and encouraging participation in social and economic activity in cyberspace. Many people fear that efforts to secure cyberspace, especially government efforts, will undermine the Internet's spirit of openness and unconstrained freedom, which is a driver of innovation. However, security enables access to an open and free cyber environment. Organizations and people will not fully engage in cyberspace and take full advantage of new technologies if they fear scams or loss of privacy. Many of these fears can be allayed if participants have faith in the security of cyberspace. Equally important, if policy is developed with input from key stakeholders across society, unwarranted fear of government involvement can be mitigated.

People

The human dimension of cybersecurity is critical, encompassing everything from technical and leadership skills to organizational culture and communications. Even the most technologically secure systems can be vulnerable to attacks that target the human dimension. When persistent adversaries are stopped by technological defenses, they often turn to social engineering attacks, which exploit human vulnerabilities. To succeed and outpace the competition in cyberspace, organizations must be able to identify, recruit, develop, and retain a cyber-aware, cyber-ready workforce that can understand and adapt to cyber threats, as well as drive innovation in cyberspace.

As governments and businesses in the Gulf focus on modernizing their workforces and empowering their citizens, one of the challenges they face is to attract, train, and engage next-generation cyber professionals who are technologically savvy and possess the dynamic problem-solving skills needed to provide the complex, multidimensional solutions required in the digital age. The first step in developing an indigenous cyber workforce is providing the education necessary to manage and implement new technologies and systems. Basic science, technology, and mathematics skills are essential to create sufficient expertise and managerial acumen to handle increasingly sophisticated technology and complex networks. Governments and businesses should partner with universities to enhance opportunities for students in cyber-related fields. Workforce planning is essential to long-term success in cyberspace and the creation of a new generation of capable citizens who can propel economic growth.

Operations

With increasing reliance on digital technologies and cyberspace to conduct daily functions and support activities, organizations must adopt a comprehensive view of their cyber operations. Narrowly focused measures aimed at keeping cyber intruders out through technology alone are unlikely to succeed against increasingly adaptive and innovative adversaries. Organizations must be able to anticipate new threats—not just react after attacks—and look beyond IT management to protect assets, reputation, competitive advantage, financial viability, and more. In addition to technological weaknesses, persistent adversaries will attempt to find and exploit vulnerabilities across people, process, policy, and management areas as well. Layers of defense within an organization and with external partners are needed to counter these threats. Successful organizations will be proactive, dynamic, and adaptive in their approach to cyber operations. They will implement layers of defense to reduce vulnerabilities across all areas and will have plans in place to effectively respond to attacks and allow for continuity of critical functions.

Technology

While point solutions such as firewalls, antivirus software, and intrusion detection are essential to secure cyber operations, true security in cyberspace requires a comprehensive approach to technology. Understanding the capabilities and limitations of current technologies and the impact of technological changes is critical to an organization's success in cyberspace. Awareness and smooth integration of emerging technologies allow an organization to stay a step ahead of adversaries. Technological solutions should be reliable, resilient, modular, interoperable, and scalable. Ultimately, organizations should use technology to allow cyberspace to be a secure and amplifying conduit for successful operations.

Evolving digital infrastructure must be cost effective and relevant to local needs. Smart devices will help accelerate the growth of data from 100 petabytes in 1990 to more than 3,000 exabytes by 2020, growing at a compound annual growth rate of over 50 percent a year and creating a data tsunami in the process. The ability to manage vast amounts of data will be critical to security and economic competitiveness.

Next-generation cyber network development includes the rapid migration of information to the cloud, resulting in improved efficiencies, reduced costs, and significant return on investment. The predictive analytics capabilities and intelligence resources available in the cloud help organizations and governments gain insights to effectively secure intellectual property and critical infrastructure. Companies trying to navigate a course amidst constantly evolving cloud-based services demand more than a vendor solution. Enterprises and governments are challenged to determine how to most effectively access, process, analyze, manage, and secure data while transitioning systems and infrastructure to the cloud environment.

Management

A holistic approach to managing the interdependent elements that comprise cybersecurity—policy, people, technology, and operations—is the key aspect to ensuring that an organization's cybersecurity and cyber operations are aligned with its broader objectives. Organizations are constantly faced with the dilemma of distributing limited resources. Leaders should prioritize cybersecurity investments and resources based on their value to the organization's business and mission. Effective management will ensure that collaboration and integration among key stakeholders are present throughout all of the dimensions of cybersecurity, as well as recognize that cybersecurity is not an end that can be achieved and then disregarded, but rather a constantly evolving path that must be proactively managed.

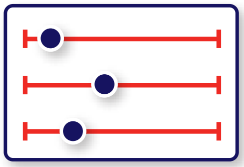
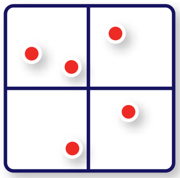
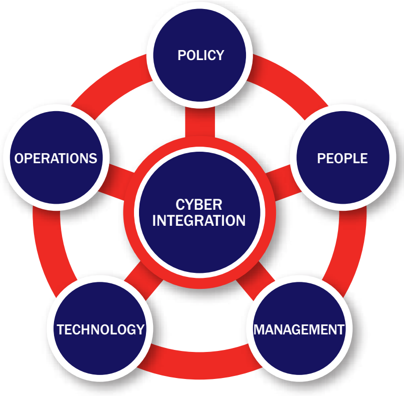
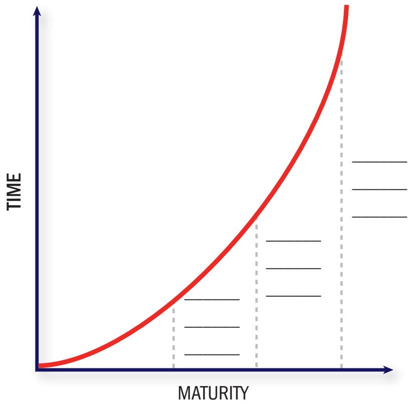
Building a Trusted and Secure Environment

Today's complex cyber domain, comprised of millions of interconnected digital pathways, dictates that many issues relating to governance, standards, research and development, and security be addressed multilaterally among global stakeholders. A collaborative approach is necessary to capture the full potential afforded to all by cyberspace. Much like the world's financial systems are governed by laws and contracts that establish the faith and trust necessary for secure transactions, cyberspace must be governed by policies and controls that establish the credibility necessary for people and organizations to confidently engage in social and economic activity.

In addition to developing a holistic cyber integration strategy to enhance cyber capabilities, emerging trends in today's threat environment require a dynamic and comprehensive operational framework for effectively measuring, managing, and maturing cybersecurity, as illustrated in Exhibit 3. The increased frequency and sophistication of cyber attacks by powerful adversaries demand coordinated policies, streamlined processes and safeguards to protect nations and their citizens, as well as the global economy.

The first step involves ***measuring*** current and anticipated cyber risks to a nation's government, businesses, and society, as well as the current capabilities to mitigate threats. This first phase sets the stage for diagnosing the maturity of security programs through the establishment of appropriate intelligence-gathering and performance management architectures.

Exhibit 3 | Measuring, Managing, and Maturing Cybersecurity

	MEASURING	MANAGING	MATURING
	 Capability Maturity Evaluation  Risk Analysis	 POLICY PEOPLE MANAGEMENT TECHNOLOGY OPERATIONS CYBER INTEGRATION	
ACTIONS	• Gain situational awareness of operating environment • Acquire threat intelligence • Evaluate security capabilities • Determine risks • Set maturity targets	• Define new projects with all cyber integration pillars in mind • Allocate and manage resources to best fill maturity gaps • Ensure performance management mechanisms are in place	• Evolve capabilities commensurate with risk environment • Continually enhance transparency and capability cross-leveraging across Government, private sector and society

Source: Booz Allen Hamilton

Cybersecurity capabilities can be effectively ***managed*** by prioritizing information assets and proportionally allocating and aligning security controls to critical, high-risk areas, thereby closing the most dangerous gaps often penetrated by today's skilled perpetrators. The most critical assets require prioritized protection based on their value creation and information sensitivity. Effective cybersecurity management practices carefully define the areas to protect and then align applicable security measures based on risk. It is important to dedicate resources to fighting the threats that will have the greatest potential negative impact. The foundation of the management principle is the implementation of an appropriate risk management architecture that includes transparency into the business and broad stakeholder participation.

Since the cyber environment is the conduit for all organizational functions, cybersecurity best practices must be implemented throughout all the people, process, and technology dimensions of the enterprise. Cyberspace continues to evolve and new technologies are constantly emerging. A successful cyber strategy will include processes for ***maturing*** the various cybersecurity disciplines within an organization, based on business needs and the risk environment. While providing periodic technological improvements based on the threat environment is necessary, maturing goes well beyond simply installing new versions of software or purchasing an upgraded firewall. Successful organizations place equal emphasis on ensuring that people skills and organizational processes are also at an appropriate level of maturity. This especially includes providing security personnel and users with appropriate education and training.

Measuring, managing, and ***maturing*** are not parts of a one-time journey, but fundamental elements of a cyclical process that serves as a roadmap for effective cybersecurity in a rapidly evolving digital world.

Conclusion

The dynamic expansion of digital, mobile, broadband, and networked communications in the Gulf region is exciting and daunting at the same time. Economic growth is accelerating as a result of increased access to advanced communications and the global network, and the GCC states are quickly becoming global hubs in transportation, finance, and communications. However, this growth introduces increased cybersecurity risks. GCC states are already experiencing significant cybercrime. They are also increasingly targeted by dangerous Internet viruses designed to disable or destroy critical infrastructures.

The most effective response to these trends is to strive for a balance between efficiency and security in telecommunications and data networks through the creation of a collaborative approach with input from key stakeholders. GCC governments are increasingly concerned about cyber threats and are beginning to take action. Efforts are underway to combat infiltration of sensitive intelligence data and protect critical infrastructures, counter the theft of intellectual property and technology trade secrets, and provide protection for government, corporate, and individual data.

The path to success lies in a comprehensive approach that enables stakeholders to collaborate in addressing shared, multidimensional cyber issues. All facets of the cyber domain must be considered: technology and standards, policy and governance, leadership and culture, planning and operations, and management and budgeting. GCC leaders who successfully collaborate with key stakeholders to create an integrated vision for cyberspace will help ensure continued economic growth in the region, and will establish a global standard for other developing regions to emulate.

Nations with a technological advantage will not necessarily wield the greatest cyber strength. Effectively maximizing capabilities in cyberspace requires the savvy integration of many elements. Countries and nation states that strategically use information and communications technologies to spur economic growth, empower civil society, and enhance national security will maximize the long-term benefits of cyber strength. Those that successfully adopt cyber technologies and integrate them into daily government, business and social environments while simultaneously recognizing and mitigating threats will emerge as prosperous and powerful leaders on the world stage.

Booz | Allen | Hamilton

About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for nearly a century. Today, Booz Allen is a leading provider of management and technology consulting services to the US government in defense, intelligence, and civil markets, and to major corporations, institutions, and not-for-profit organizations. In the commercial sector, the firm focuses on leveraging its existing expertise for clients in the financial services, healthcare, and energy markets, and to international clients in the Middle East. Booz Allen offers clients deep functional knowledge spanning strategy and organization, engineering and operations, technology, and analytics—which it combines with specialized expertise in clients' mission and domain areas to help solve their toughest problems.

The firm's management consulting heritage is the basis for its unique collaborative culture and operating model, enabling Booz Allen to anticipate needs and opportunities, rapidly deploy talent and resources, and deliver enduring results. By combining a consultant's problem-solving orientation with deep technical knowledge and strong execution, Booz Allen helps clients achieve success in their most critical missions—as evidenced by the firm's many client relationships that span decades. Booz Allen helps shape thinking and prepare for future developments in areas of national importance, including cybersecurity, homeland security, healthcare, and information technology.

Booz Allen is headquartered in McLean, Virginia, employs approximately 25,000 people, and had revenue of $5.86 billion for the 12 months ended March 31, 2012. *Fortune* has named Booz Allen one of its "100 Best Companies to Work For" for eight consecutive years. *Working Mother* has ranked the firm among its "100 Best Companies for Working Mothers" annually since 1999. More information is available at www.boozallen.com. (NYSE: BAH)

To learn more about the firm and to download digital versions of this article and other Booz Allen Hamilton publications, visit www.boozallen.com.

Contact Information:

Roger Cressey
Senior Vice President
cressey_roger@bah.com
703-984-1421

Mahir Nayfeh
Vice President
nayfeh_mahir@bah.com
+971-2-656-5808

Booz | Allen | Hamilton

Principal Offices

Huntsville, Alabama

Sierra Vista, Arizona

Los Angeles, California

San Diego, California

San Francisco, California

Colorado Springs, Colorado

Denver, Colorado

District of Columbia

Orlando, Florida

Pensacola, Florida

Sarasota, Florida

Tampa, Florida

Atlanta, Georgia

Honolulu, Hawaii

O’Fallon, Illinois

Indianapolis, Indiana

Leavenworth, Kansas

Aberdeen, Maryland

Annapolis Junction, Maryland

Hanover, Maryland

Lexington Park, Maryland

Linthicum, Maryland

Rockville, Maryland

Troy, Michigan

Kansas City, Missouri

Omaha, Nebraska

Red Bank, New Jersey

New York, New York

Rome, New York

Dayton, Ohio

Philadelphia, Pennsylvania

Charleston, South Carolina

Houston, Texas

San Antonio, Texas

Abu Dhabi, United Arab Emirates

Alexandria, Virginia

Arlington, Virginia

Chantilly, Virginia

Charlottesville, Virginia

Falls Church, Virginia

Herndon, Virginia

McLean, Virginia

Norfolk, Virginia

Stafford, Virginia

Seattle, Washington

The most complete, recent list of offices and their addresses and telephone numbers can be found on www.boozallen.com