A SAUDI OUTLOOK FOR CYBERSECURITY STRATEGIES

EXTRAPOLATED FROM WESTERN EXPERIENCE

By NAEF BIN AHMED AL-SAUD

In the 21st century, countries across the globe have come to rely on complex computer networks that form the infrastructural backbone of even the most basic necessities of life, including electric power grids, global finance, food distribution, medical care, clean drinking water, petroleum production, and most types of communication. The protection of such networks, known as *cybersecurity*, is among the highest priorities in the civilized world, alongside planning and operations for major contingencies, including antiterrorism and land warfare.

In many countries, given the typical mandate for militaries to protect civilian infrastructure from physical attack, cybersecurity responsibilities divided between military and civilian leadership structures appear to overlap and cause confusion, particularly in times of crisis. Cybersecurity encompasses some of the most vital national security issues that may be faced by top civilian leaders and military commanders from the United States, as well as the North Atlantic Treaty Organization (NATO) and other friendly nations—especially including Saudi Arabia, which is located in one of the world's most strategic energy resource regions.

The Saudi understanding of cybersecurity is largely derived from the American and European experience in such deployments, both defensively and counteroffensively. Saudi Arabia aims to develop a deeper understanding of the American and Western policy formulation and decisionmaking experiences that are relevant to those top leaders in the Kingdom who are concerned with such vital defense parameters. Thus, it is necessary to observe the strengths and perceived vulnerabilities, as well as the proactive measures, of the United States and other Western nations in response to incidents and intrusions and to analyze them in terms of long-term cybersecurity development considerations pertaining to the Kingdom. Therefore, this article discusses recent developments; U.S. cyberstrategy mission implications for the Kingdom; future development factors toward indigenous Saudi multibillion-dollar investments in cybersecurity infrastructure, institutions, and support services; and the need for substantial long-term Saudi funding—corresponding to Saudi high employment levels in cybersecurity, which are directly related to credible national security objectives and defenses against real-world threats.

Recent Developments

In the aftermath of the successful U.S. special operations force mission in Abbottabad, Michael Clarke, director of the Royal United Services Institute in London, observed that "we are getting close to the Hollywoodesque situation in which a U.S. president might be in a position to direct an operation tactically at the lowest levels."[1] The world's most advanced armies are converging military special operations with advanced technology over ultra-complex networks that must be protected by effective cybersecurity, and Saudi Arabia aims to be among those in

the Saudi understanding of cybersecurity is largely derived from the American and European experience

His Royal Highness Brigadier General Naef Bin Ahmed Al-Saud of the Royal Saudi Army holds a doctorate from Cambridge University and is a graduate of the National War College. His professional focus includes military special operations and international diplomacy.

the forefront, while gaining from the experiences of its friends and allies in the West.

What factors determine when a particular cyberwar starts or ends? International experts in cybersecurity do not seem to fully agree, so it is challenging for government policymakers to understand all of the pertinent criteria for making decisions.[2] In November 2010, General Keith Alexander, commander of U.S. Cyber Command (USCYBERCOM), told Congress that the engagement rules were not clear about what sort of cyber attack would precipitate a U.S. response.[3] These unknown factors trigger other directly related parameters. Western government institutions such as USCYBERCOM and the United Kingdom's Cyber Security Operations Centre are intended to protect the military and the government.[4] Yet as stated in a November 2010 Chatham House report, *On Cyber Warfare*, "In cyberwarfare, the boundaries are blurred between the military and the civilian, the physical and the virtual, and power can be exerted by states or non-state actors, or by proxy." Experts indicate that economic dynamics underpinning cyberspace conflicts may directly impact the way wars are fought in the future. The Chatham House report further points out that "in cyberwarfare it is extremely difficult to direct precise and proportionate force; the target could be military, industrial or civilian."[5] Accordingly, Saudi Arabia would like to know more about Western defense planning against national security damage due to attacks on civilian industries vital to national security, such as banking, electricity, and energy.

In March 2011, an Internet company, EMC's RSA Security, which provides the heavily used SecurID system to U.S. Federal agencies including the Department of Defense (DOD), found "certain information" had been "extracted."[6] According to the company, this type of information theft could result in a subsequent successful attack.[7] Since RSA has multimillion-dollar contracts to provide DOD with network security, Saudi Arabia may prefer to find out more about whether USCYBERCOM stepped in immediately, or the private company's own experts retained the lead in defensive maneuvers and offensive countermaneuvers. These matters would help to address the lines of support between military and civilian cybersecurity defense responsibilities as well. Such insights may have critical impacts on development of the Kingdom's own cybersecurity capabilities under Saudi government coordination, with significant potential assistance from USCYBERCOM and top international private specialists.

trillions of dollars of Gulf-derived petroleum transactions will continue to be recorded via the computer networks of the financial world

Lieutenant General Rhett Hernandez, commander of U.S. Army Cyber Command, indicates that cloud computing could reduce many risks from decentralized hosted systems, though other increased risks may appear if networks with greater centralization are hacked, thus highlighting the need to achieve "the right balance between centralization and decentralization."[8] Coincidentally, such balanced wisdom of spreading work beyond single sources was reinforced by the April 2011 reports of large-scale cloud computing data breaches at some of the largest global private enterprises, Sony and Amazon.[9]

Analogously, civilian government cyberdefenses have also been routinely breached. In late March 2011, the European Union headquarters was subjected to a significant cyber attack that appeared to be state-sponsored. It occurred right before the start of the European Union Summit.[10] According to Patrick Pailloux, director general of the French National Agency for Information Systems Security, "No single infrastructure system is safe enough."[11] In early March 2011, the French government was the victim of a cyber attack that accessed and spied on numerous classified documents on roughly 150 computers in the French finance ministry with what would appear to be sensitive details about international aspects of France's economic policy.[12] This took place before the Group of 20 nations were to meet under French leadership.

In a related context to economic policy, some Western experts appear deeply concerned that there is "not much, if any, cyber-war defense planning going on in the financial world" and possibly insufficient protection for stock exchanges or financial institutions if they come under cyber attack.[13] National security incidents pertaining to international economics and finance are no joke. The 2007 cyber attack launched against Estonia and its two primary banks, possibly by another state, still resonates as a glaring example of how a country's banking and financial services may be shut down for many days or longer. One reported concern could include "Stuxnet-type worms that might be insinuated into financial networks. Such worms can wreak havoc slowly and methodically by corrupting financial data without creating immediate alarm."[14]

These types of issues pertaining to international finance may turn out to be directly relevant to Saudi national interests since a large proportion of sovereign assets intended to be invested toward securing the future of Saudi citizens are held in instruments traded on global financial markets, often in the custody of major international financial institutions. Over the long term, trillions of dollars of Gulf-derived petroleum transactions will continue to be recorded via the computer networks of the financial world. Hypothetical vulnerabilities in Western cyberwarfare defense plans might not remain a perpetual abstraction to America and the West, or to the Kingdom and regional governments, in proactive protection of their citizens.

Roughly analogous infrastructural attack scenarios could also apply to petroleum pumping stations, shipping, and other assets in the Gulf region. Gulf governments may therefore contemplate some hypothetical developments, such as rogue international oil brokers outside the Gulf region who could conceivably hire hackers to interfere with the petroleum infrastructure while betting on oil price trends. That could damage the credibility of large sectors of global financial markets.

The Kingdom and other Gulf countries may want to consider how to determine when USCYBERCOM would make the decision to focus its resources—whether before or after invitation by Gulf governments—and how the chains of command would intersect among sovereign nations and allies. Tangentially, as former Defense Secretary Robert Gates reflected concerning NATO, "On cybersecurity, the alliance is far behind. . . . Our vulnerabilities are well known, but our existing programs to remedy these weaknesses are inadequate."[15] Basically, the Secretary made it clear that there are serious weaknesses in NATO's computer network defenses—throughout the command structure. Thus, Saudi Arabia is highly interested in observing what transpires in Washington, so the Kingdom does not find itself needing


Saudi soldiers train to enter and search building during exercise Friendship Two, Forward Operating Base Sumter, Saudi Arabia

U.S. Army (Erica Knight)

the American President and Congress may need to clarify laws and policies to permit the U.S. military to protect critical infrastructure

to reinvent the wheel by revisiting cybersecurity bottlenecks that may be resolved by the United States. As a result, the Kingdom may also wish to pursue regulations toward financial incentives for Saudi businesses to invest—indigenously—in the Kingdom's own large and growing needs for cybersecurity as well as in a private Saudi cyber insurance industry, with rules supporting responsibilities between the Ministry of the Interior and Ministry of Defense along with the Kingdom's other institutions.

Pentagon Cyberstrategy Mission Implications for the Kingdom

Most of the U.S. Government's computer networks may be presumed to be under Pentagon control,[16] while most of the important economic targets to be defended are inside the United States, such as financial networks, hydro infrastructure, electrical power grids, and petroleum and other energy distribution. Saudi Arabia would like to learn about the experience that America derived from defending such vital economic infrastructure from cyber attacks in order to maximize its own effective management responsibilities concerning the government's computer systems and the Kingdom's economic targets.

Under rules announced in October 2010, President Barack Obama approved using the U.S. military's cyberwarfare expertise if computer networks are attacked inside the United States and the Department of Homeland security directs the work.[17] Lieutenant General Hernandez points out:

Cyber Command is responsible for the defense of the dot-mil domain space and when directed to do so, to support the Department of Homeland Security in defending [America's] *critical infrastructure. Cyber Command uses a defense in depth approach that is executed by each of our Armed Services. . . . This defense against cyberwarfare is focused on DOD infrastructure.*[18]

According to the January 2011 cybersecurity report issued by the Center for Strategic and International Studies (CSIS), the American President and Congress may need to clarify laws and policies to permit the U.S. military to protect critical infrastructure.[19] In May 2011, 2 years after President Obama declared that even American nongovernmental computer networks are strategic national assets, the White House released a new proposal for cybersecurity laws that would require industries crucial to America's security and economy to ensure that their computer systems are secure. The proposed laws also encourage greater access for public and private businesses to consult with the Department of Homeland Security, which provides cybersecurity for the U.S. Government's nonmilitary computer systems.[20] Coincidentally and fortuitously, like the Kingdom's top leadership, U.S. Congressmen still appear to be interested in finding out more concerning how USCYBERCOM would meet its broad mission, given the extent of serious vulnerabilities in cyberspace.[21] Similarly, Saudi Arabia would like to consider the coordination of responsibilities between the Saudi Ministry of Defense and other security institutions, along with computer systems of vital economic targets, which may deserve national security protective designation inside the Kingdom.

With such issues in mind, former Deputy Secretary of Defense William Lynn pointed out that in 2008 a foreign intelligence agent deployed a flash drive in order to affect U.S. military computers including those used by U.S. Central Command to manage combat in Afghanistan and Iraq.[22] According to Lynn, "It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown enemy." The Pentagon's response was Operation *Buckshot Yankee*, which was a turning point for America's strategy toward cyberdefense.[23] This means that Middle East battlefield experiences may have been crucial in redirecting the U.S. military toward cyberdefense.

Deputy Secretary Lynn observed that if only a dozen computer programmers find a vulnerability, they can threaten America's global logistics network, steal operational plans, damage intelligence-gathering, and interfere with the delivery of weapons to their targets.[24] By now, national defense institutions recognize that cyber combat is another form of devastating asymmetrical warfare, potentially resulting in large casualties inflicted by "rogue warriors" who do not need a false religious ideology to coordinate and create chaos for the civilized world. Deputy Secretary Lynn reassured readers that the United States has developed systems against intrusion that are "part sensor, part sentry, part sharpshooter."[25] Thus, it may be highly relevant for the top brass in Gulf defense ministries to receive additional insights from other friendly military institutions, particularly USCYBERCOM, about effective track records of such systems' deployment in order to be equipped to confidently report back to the senior leadership echelons in Gulf governments. Lynn revealed that many intrusions are more like espionage than acts of war.[26] Saudi Arabia would like to

find out more about the criteria the United States considers as it coordinates responsibility for various intrusions between intelligence institutions and defense resources.

Deputy Secretary Lynn indicated that deterrence may need to be focused on denying benefits to the attackers rather than retaliating. This is due to the typical pattern of hackers designing attacks by compromising servers in neutral countries.[27] Here is a hypothetical scenario that is of serious interest to Saudi Arabia. If hackers were to compromise servers in a neutral country in order to interfere with Aramco computer systems, it could be considered a Saudi national security threat—perhaps roughly analogous to the U.S. national security threat of aggregated large-scale, offshore, tax-based fraud against the U.S. Treasury.[28] If the Kingdom were to request assistance from the United States and other friendly countries, it could possibly be at the time of the incident—or the principals might prefer that a preexisting agreement would already be in force between the countries. The Kingdom may aim to discover more about some main factors used to measure how intrusive U.S. or other foreign country assistance would tend to be toward Saudi civilian and military computer systems, whether incident-by-incident or under preexisting agreement.

The former Deputy Secretary observed that military supply lines involving private companies often require defense institutions to use basically unclassified networks on the open Internet.[29] Military analogies to related civilian experiences may be appropriate, as DOD has detected counterfeit hardware in its procurement programs.[30] Microsoft and other companies have been working on "risk-mitigation strategies" against dangerous codes to keep them out of global supply chains, and Lynn made it clear that the U.S. Government needs to do the same.[31] The United States and Saudi Arabia also acquire weapons systems and supplies from other countries. The Kingdom would like to know more about how the U.S. military's global supply chains, reaching to other countries, may be deemed subject to effective "risk mitigation strategies." Ultimately, America's military global supply chains directly affect the Kingdom, which is negotiating to purchase complex American weapons systems worth up to tens of billions of dollars, presumably incorporating highly relevant proportions of components from private industry vendors. According to the Western media, the Kingdom is deemed to be the largest purchaser of American arms.[32]

there may be countries—specifically India and China—that will train more capable computer scientists than the United States

Saudi King Abdullah bin Abdul-Aziz Al-Saud

DOD (Flickr)

In this context, the Ministry of Defense was highly interested in the Defense Advanced Research Projects Agency's research on identifying rogue microchips, as well as in outcomes from the U.S. Army Research Office conference dealing with "kill switches" in 2011.[33] The direct relevance to the Kingdom's cybersecurity of kill switches, which may be routinely manufactured within microchips, includes the potential for remotely shutting down computer networks or weapons systems controlled by computer networks, whether they are linked to the Internet or accessed from radio signals via extremely small antennas that may be easily hidden and are virtually undetectable within the microchips.[34]

Such issues are important to the Kingdom since it faces its own unique threats, including anti-Islamic terrorists and copycats. Here is just one basic scenario. In the Stuxnet incident, Western cybersecurity experts may appear to have detected a hidden Hebrew reference.[35] Building on that, if native Arabic-speaking hackers were to use "trap doors" or other methods encrypted by references to aspects of Arab culture, leading to logic programming patterns for which Western encryption experts may not grasp the full implications, Saudi cyberwarriors and other Arab experts would need to be the ones providing such highly specific guidance to friendly governments.

In terms of non-Western cultures, Deputy Secretary Lynn appears to indicate that over the next couple of decades there may be countries—specifically India and China—that will train more capable computer scientists than the United States.[36] Therefore, Arab computer scientists should also be recognized as among the world's best.

This is the dawn of a new century, a time when cybersecurity will be absolutely vital to the national security of civilized nations. Therefore, it is extremely important to note that, centuries ago, the Arab world gave Western civilization higher mathematics and science. Neither computer technology nor the Internet could exist without those gifts from Arab minds. Today, contemporary Arab minds also claim the international respect they deserve. We should be confident that Arab talents are fully

available. A significant proportion of such vital economic output should be created by Arab minds, particularly including the Kingdom. In coming years, cybersecurity is likely to be worth billions of dollars in the defense budgets of Gulf countries, and possibly tens of billions of dollars or more.

Another absolutely relevant factor is that extensive employment in high technology may need to be among the vital objectives of Saudi economic planning, and particularly its national security objectives. Saudi Arabia aims to encourage the United States and other friendly governments to work with the region toward these results.

Now we must focus on the other side of the equation—where threats originate. If native Arab-speaking hackers are involved in cyber attacks, it may make sense not only to neutralize the system vulnerabilities by which they entered, but also to recruit the bad guys by "flipping" them to the side of the good guys. Consider a brief case study involving Google, one of the world's most respected Internet companies, which has suffered severe cyber attacks originating from both inside and outside the United States. Some reports even suggest that one or more foreign governments may have been behind the attacks on Google's computers. So the company appears to have made it a point to recruit individuals with hacking talents in order to strengthen its own defenses. Obviously, Google follows Sun Tzu's advice: "Keep your friends close and your enemies closer."

The Kingdom would also look to flip Arab hackers, particularly given extensive positive Saudi experience in keeping friends close and enemies closer. This theme is consistent with Saudi Arabia's successful rehabilitation program for former radical militants. It is likely that U.S. Cyber Command may have significant opportunities to rehabilitate Western hackers, if they are identified, by offering them legitimate employment—potentially in hunting down other hackers. This is the 21st-century cybersecurity version of "Set a thief to catch a thief." The Kingdom will likely be willing to share its own highly successful technical and psychological insights in flipping troublemakers with USCYBERCOM and institutions such as the National Defense University.

Future Development Factors

The top Western and other international information technology (IT) corporations already have a significant presence in the Kingdom and have helped to set up highly sophisticated computer networks for the country's defense and economic infrastructure including electric power grids, water supplies, oilfield maintenance, and petroleum pipelines to shipping terminals. They have years of significant experience dealing with "soft power" factors such as Saudi institutions and culture, as well as other critical issues. Those IT corporations may be a major source of insight—both for and from—the Saudi government, including the Ministry of Defense.

So in terms of evolving and achieving particular objectives in cybersecurity and information assurance, the Kingdom's leadership may consider numerous multibillion-dollar options over the long term, possibly including:

- direct discussions with major international corporations with significant cybersecurity backgrounds
- close cooperation with USCYBERCOM, possibly roughly analogous to programs run by the U.S. Government for foreign military sales at the acquiring country's request
- training programs and other considerations that may be provided by institutions such as the National Defense University
- a hybrid approach involving iterations of these options.

To attain the necessary manpower objectives to secure superlative cybersecurity expertise, Saudi Arabia may encounter challenges similar to those already faced by America and the West. A November 2010 report by the Center for Strategic and International Studies made it clear that the United States is facing a severe shortage of skilled cybersecurity experts. According to Central Intelligence Agency Clandestine IT Office founding director Jim Gosler, the United States has only around 1,000 cybersecurity experts with sufficiently high skills, while 10,000 to 30,000 are needed.[37] This may mean that, extrapolating from relative population sizes, the Kingdom may need to train up to 3,000 Saudi cybersecurity experts with the highest skills and experience—in addition to addressing potential future needs for tens of thousands of trained Saudi cybersecurity personnel for basic compliance matters.

The CSIS report further indicates that although cybersecurity is a growing field, only some of its practitioners "know what they are doing."[38] Accordingly, in the United States, "the current professional certification regime is not only merely inadequate; it creates a dangerously false sense of security" for reasons that include credentials that demonstrate expertise in documentation of compliance with statutes and policy, in contrast to far more sophisticated expertise in preventing attacks, responding to them, and mitigating risks.[39] Western commentators have suggested that cybersecurity credentials may need to go beyond professional certification toward licensing and thereby subjecting the field to regulation, so service buyers are more able to evaluate what they would be acquiring.[40] Given such difficulty in evaluation, Saudi Arabia may need to pay careful attention to the highly significant difference between the cyber elite—including "hunters" who are able to look deep into computer networks, tracking attackers[41]—and the Kingdom's future tens of thousands of substantially less qualified "certification" graduates, who may turn out to be quite suitable and necessary for roles in cyber compliance and cyber documentation, but are not fully qualified as "cyber-warriors"[42] (and other descriptive accolades) for responding to cyber attacks.

The November 2010 CSIS report stated that in cybersecurity:

Most importantly, training and certifications need to be connected to real jobs in the current marketplace [and] *new challenges. This criterion also recognizes it will take time to implement the model. . . . Potential employers and purchasers of cyber security services need to be assured that certification processes have intellectual rigor and are not unduly biased by the economic interests of particular providers.*[43]

international information technology corporations have years of significant experience dealing with "soft power" factors such as Saudi institutions and culture

Such direct implications for Saudi Arabia, as for the United States and the West, are that real-world job requirements and cyber challenges may need to dictate higher parameters of training, certification, and so on, rather than merely assuming that training or certification would conversely meet real-world

job requirements. After all, in the Kingdom as well as in America and the West, unemployment and unsuitability for real-world employment are major policy concerns that need to be addressed by real-world solutions—not only in the growing realm of cybersecurity, but also throughout the respective economies.

The CSIS report makes clear that those who exploit weaknesses by launching cyber attacks against America (and presumably other civilized countries in the West and elsewhere across the globe) "are every bit as smart as we are"[44]—and "while much is being done, our adversaries are growing in number and capability. We must redouble our efforts."[45] Nonetheless, the CSIS report may have inadvertently overlooked the reality that adversaries—against America, the West, the Kingdom, and other countries—may often be top-down thinkers rather than bottom-up graduates of certification courses, licensing regulation, or other more structured and more sophisticated cybersecurity career paths. The CSIS report recommends cybersecurity career trajectories apparently like those of medical careers and specializations, with clear skill sets that may be more effectively evaluated by those who need to purchase medical or, analogously, cybersecurity services.[46]

However, the CSIS medical analogy may not necessarily resolve the most crucial cybersecurity concerns. Medical doctors tend to learn by rote memorization and repeated procedures; the typical (even complex) problems that patients go to medical specialists for are usually not unique. Doctors typically apply their understanding as derived from numerous other cases and case studies to prescribe solutions that worked for patients before. By contrast, in cybersecurity and cyberwarfare, many attacks intended to be the most devastating may be designed to be unique. Stuxnet is a good example. Therefore, one problem with streamlining cybersecurity careers by certification and licensing regimes is that it may inadvertently create vulnerabilities in civilized governments because cybersecurity personnel may be vulnerable to thinking alike, or "groupthink." By contrast, as in nature, cross-breeding tends to improve the stock. It would appear that international cyberterrorists who launch damaging cyber attacks tend to be mavericks, intentionally outmaneuvering those with more structured backgrounds, methods, and thinking patterns, and their potential devastation may have something to do with the notion that they did not necessarily start by graduating from certification or licensing programs with oversight boards that may inadvertently encourage structured thinking "inside the box."

in cybersecurity and cyberwarfare, many attacks intended to be the most devastating may be designed to be unique

Conclusion

Cybersecurity is a fundamental national security priority for the United States as well as allies and friends including NATO and Saudi Arabia. One Western observer pointed out that just a few years ago, only militaries had large weapons systems capable of causing large-scale damage—but now, anybody with enough computer skills can create chaos within major economies.[47] Western experts indicate that the world's next arms race may be about computer codes instead of firepower.[48] For numerous reasons—including the probability that the fate of the global economy relies on Saudi Arabia, which heavily deploys computer networks to maintain productivity in one of the world's most strategic energy producing regions—strong commitment to Saudi cybersecurity is paramount.

To reiterate, Robert Gates recognized that existing programs to address cybersecurity vulnerabilities are not adequate.[49] His observation was made in the context of the American alliance with NATO computer network defenses, and may also pertain to other friendly nations including Saudi Arabia. In recent years, vital infrastructural areas of the United States and European countries appear to have been attacked by other nations, which in some instances may have attempted to hide "trap doors" and other dangerous vulnerabilities for future cyber assaults. Cyber attacks may grow at accelerated rates with increasing scales of potential destruction.

In the United States, it would appear that most government computer networks may be within DOD jurisdiction,[50] while many vital economic infrastructural networks tend to be under separate civilian government or private control, whether supporting financial institutions, water distribution and treatment facilities, electric power grids, petroleum and other energy transportation, or other enterprises. The Kingdom, along with other friendly nations including NATO, will need to understand more about the lines of demarcation in the United States and the West between civilian and military cybersecurity responsibilities for defending such economic networks and their international links.

Such international links elicit recognition that, according to former Deputy Defense Secretary Lynn, in the near future many countries, including China and India, may produce more highly trained computer scientists than the United States.[51] Likewise, Arab minds and Arab talents deserve recognition. If emerging regions may produce significant numbers of computer scientists, they may also be sources of cyber attacks. The Middle East and particularly the Gulf may remain a significant concern for international cyberwarfare—particularly in the aftermath of Stuxnet and its possible hidden programming reference to foreign (non-Western) culture. Legitimate Saudi and other Arab cyber talent will need to become even more focused in this global arena—for reasons that include the reality that many

Marine Chief of Training and Advisor Group and member of Royal Saudi Naval Forces meet at Camp Geiger, School of Infantry–East

U.S. Marine Corps (Maxton G. Musselman)

future cyber threats may require indigenous Saudi and other Arab expertise since the ulterior significance of such threats may not be fully understood by Western or other non-Arab experts. A substantial percentage of world trade, including energy supplies, is transacted through the Kingdom and may therefore require multibillion-dollar, long-term investments in Saudi cybersecurity.

Nonetheless, American and other Western experts cited in media reports have made clear that a significant proportion of Western cybersecurity practitioners does not necessarily appear to know what it is doing in terms of addressing major threats, even though many may be graduates of certification programs.[52] Therefore, a major government policy challenge for Saudi government institutions will be to acquire a deep understanding of the American and Western experience to ensure that such large investments in cybersecurity infrastructure, institutions, and support services are not merely theoretical but must be directly related to pragmatic job skills deployable as measurable assets against real-world cybersecurity threats. The tremendous investment potential for sophisticated indigenous multibillion-dollar cybersecurity requirements, which should fuel Saudi high employment in such ultra-high technology, may deserve to be an integral national security objective of the Kingdom's long-term economic plans. **JFQ**

if emerging regions may produce significant numbers of computer scientists, they may also be sources of cyber attacks

His Royal Highness Prince Naef Bin Ahmed Al-Saud would like to recognize I.K. (Asa) Sabbagh, Jr., for his research, analysis, and other significant contributions in drafting this article.

NOTES

[1] Royal United Services Institute Director Michael Clarke, quoted by Daniel Dombey, James Blitz, and Peter Spiegel, "Warfare: An advancing front," *Financial Times*, May 9, 2011.

[2] Bruce Schneier, "It will soon be too late to stop the cyberwars," *Financial Times*, December 2, 2010.

[3] Joseph Menn, "Rules of engagement for cyberwars see slow progress," *Financial Times*, December 28, 2010.

[4] "How to thwart cyberwarriors," *Financial Times* (editorial), January 23, 2010.

[5] Paul Cornish et al., *On Cyber Warfare*, Chatham House Report (London: Royal Institute of International Affairs, 2010), 37, available at <www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf>.

[6] Ellen Nakashima, "U.S. Agencies respond to cyberattack on information security firm," *The Washington Post*, March 23, 2011.

[7] Ibid.

[8] Harrison Donnelly, ed., "Cyberspace in Support of Full Spectrum Operations," interview with Lieutenant General Rhett A. Hernandez, commander, U.S. Army Cyber Command, *Military Information Technology* 15, no. 3 (April 2011), 17–18, available at <www.MIT-kmi.com>.

[9] "Cloud computing's growing pains: Break-ins and breakdowns: The lessons from Sony's big security lapse and Amazon's cloud-computing outage," *The Economist*, April 28, 2011. ("Firms that use cloud-based systems should be looking at ways to distribute work across multiple providers.")

[10] Warren Getler, "Are We Ready for a Financial Cyber Attack?" *The Wall Street Journal*, March 31, 2011.

[11] Max Colchester and Gabriele Parussini, "France Investigates Attack on Computers," *The Wall Street Journal*, March 7, 2011.

[12] Ibid.

[13] Getler.

[14] Getler cites Michael Chertoff for the idea that Stuxnet-type worms could be deployed against financial networks.

[15] Thom Shanker, "Pentagon Will Help Homeland Security Department Fight Domestic Cyberattacks," *The New York Times*, October 20, 2010.

[16] Ibid.

[17] Ibid.

[18] Correspondence for attribution from U.S. Army Lieutenant General Rhett A. Hernandez to author, April 20, 2011.

[19] Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency, *Cybersecurity Two Years Later* (Washington, DC: CSIS, January 2011), 10, available at <http://csis.org/publication/cybersecurity-two-years-later>.

[20] "Fact Sheet: Cybersecurity Legislative Proposal," Washington, DC, The White House, May 12, 2011, available at <www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal>.

[21] Thom Shanker, "Cyberwar Chief Calls for Secure Computer Network," *The New York Times*, September 23, 2010.

[22] Brian Knowlton, "Military Computer Attack Confirmed," *The New York Times*, August 25, 2010, available at <www.nytimes.com/2010/08/26/technology/26cyber.html>.

[23] Ibid.

[24] Ibid.

[25] Ibid.

[26] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* (September–October 2010), available at <www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain>.

[27] Ibid.

[28] America's own War of Independence in the latter 18th century was catalyzed by the national security imperative to fight against illegitimate siphoning of American tax dollars offshore, as demonstrated by the Boston Tea Party.

[29] Lynn.

[30] Ibid.

[31] Ibid.

[32] Craig Timberg, "Gates has 'warm' meeting with Saudi Arabia's King Abdullah," *The Washington Post*, April 5, 2011.

[33] "High-tech warfare: Something wrong with our **** chips today: Kill switches are changing the conduct and politics of war," *The Economist*, April 7, 2011.

[34] Ibid.

[35] Arthur Bright, "Clues emerge about genesis of Stuxnet worm: Biblical and historical references hint the Stuxnet worm may be of Israeli design," *Christian Science Monitor*, October 1, 2010, available at <www.csmonitor.com/World/terrorism-security/2010/1001/Clues-emerge-about-genesis-of-Stuxnet-worm>.

[36] Lynn.

[37] Karen Evans and Franklin Reeder, *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters* (Washington, DC: CSIS, November 2010), available at <http://csis.org/files/publication/101111_Evans_HumanCapital_Web.pdf>.

[38] Ibid., vi.

[39] Ibid., vi, 3.

[40] Ibid.

[41] Definition of *hunters* provided by Evans and Reeder, 2.

[42] *Cyberwarriors*, as the term is used by Evans and Reeder, 8.

[43] Ibid., 17.

[44] Ibid., 5.

[45] Ibid., 19.

[46] Ibid., 17.

[47] Schneier.

[48] Richard Falkenrath, "From Bullets to Megabytes," *The New York Times*, January 26, 2011.

[49] Thom Shanker, "Pentagon Will Help Homeland Security Department Fight Domestic Cyberattacks," *The New York Times*, October 20, 2010, available at <www.nytimes.com/2010/10/21/us/21cyber.html>.

[50] Ibid.

[51] Lynn.

[52] Evans and Reeder, vi, 3.