KINGDOM OF SAUDI ARABIA CYBER READINESS AT A GLANCE

Melissa Hathaway, Francesca Spidalieri, and Fahad Alsowailm

September 2017

POTOMAC INSTITUTE FOR POLICY STUDIES

Published by Potomac Institute for Policy Studies

Potomac Institute for Policy Studies
901 N. Stuart St, Suite 1200
Arlington, VA 22203
www.potomacinstitute.org
Telephone: 703.525.0770; Fax: 703.525.0299

Email: *CyberReadinessIndex2.0@potomacinstitute.org*

Follow us on Twitter:
@CyberReadyIndex

Cover Art by Alex Taliesen.

Acknowledgements

The authors would also like to thank Alex Taliesen for cover art and Sherry Loveless for editorial and design work.

KINGDOM OF SAUDI ARABIA
CYBER READINESS AT A GLANCE

TABLE OF CONTENTS

KINGDOM OF SAUDI ARABIA

CYBER READINESS AT A GLANCE

Country Population	31.54 million
Population Growth	2.1%
GDP at market prices (current $US)	$646.002 billion
GDP Growth	3.5%
Year Internet Introduced	1994
National Cyber Security Strategy	2013 (not published yet)
Internet Domain	.sa
Internet users per 100 users	69.6
Fixed broadband subscriptions per 100 users	11.9
Mobile cellular subscriptions per 100 users	177

Information and Communications Technology (ICT) Development and Connectivity Standing

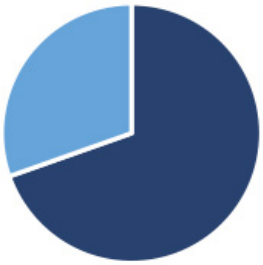
International Telecommunications Union (ITU) ICT Development Index (IDI)	**45**	World Economic Forum's Networked Readiness Index (NRI)	**33**

Sources: World Bank (2015), ITU (2016), NRI (2016), and Internet Society.

INTRODUCTION

The Internet was first introduced in the Kingdom of Saudi Arabia in 1993 as an academic project at the King Fahd University of Petroleum and Minerals (KFUPM) in Dhahran, with the first connections made available at the College of Computer Sciences and Engineering.[1] This connection used a satellite link to Bethesda, Maryland, and the limited Saudi Internet infrastructure was managed by the Washington Coordinating Center. It also hosted official Saudi government websites in the United States.[2] At that time, only email service was available to University staff due to limited international bandwidth and slow connection speed. Access to the Internet remained limited to selected staff at academic, medical, research, and government institutions through the 1990s. These organizations – almost all based in the capital of Riyadh – were using a 64kbps channel provided by the King Fahd Specialist Hospital and Research Center (KFSHRC) and administered by the King Abdulaziz City for Science and Technology (KACST) – the country's national center for science, technology, and innovation. KFSHRC was connected to the Internet via a proprietary satellite link, and KACST was linked to KFSHRC via microwave. In 1994, KACST became the manager of the country's Internet domain .sa and was tasked with coordinating all Internet services within the Kingdom.

In 1997, after several years of study and deliberations, the Saudi Council of Ministries authorized KACST to expand Internet access and services to the rest of the country. It also tasked the Saudi Telecommunications Company (STC) – at that time, a government-owned company and the sole provider of telecom services – with building the domestic infrastructure necessary to facilitate interconnection between the state-owned Internet backbone and other Internet Service Providers (ISPs). In 1998, Internet governance fell under the purview of the Internet Service Unit (ISU), a department of the KACST reporting directly to KACST Vice President for Scientific Research Support.[3] In 1999, the ISU officially opened its networks to licensed commercial ISPs, although STC remained the only ISP available in Saudi Arabia until 2005. KACST – through the ISU – became the country's single Internet exchange point and gateway between the international Internet and the national intranet.[4] The ISU controlled the country's Internet services, operated the Saudi domain name (.sa), and formulated rules and regulations to govern the use of the Internet in the country, including access control and filtering of "harmful," "illegal," "anti-Islamic," or "offensive" online material. As part of this responsibility, the ISU implemented a content control system (filtering both incoming and outgoing traffic) in order to balance its desire to facilitate public access to the Internet while at the same time ensuring the content is in line with the country's conservative values and Islamic teachings.[5]



Saudi Arabia Internet Penetration: 69.6%

Internet access became available to all citizens in the Kingdom of Saudi Arabia in 1999.

In 2003, the Saudi Communications Commission was renamed the Communications and Information Technology Commission (CTIC) and was tasked with licensing, monitoring, and filtering processes previously managed by KACST. In addition, it provides Internet access to the private sector and resolves disputes among private telecommunication companies.[6] The ISU continues to provide Internet access to government departments, as well as Saudi research and academic institutions, but Saudi Arabia is now connected to the Internet through two country-level data services providers – the Integrated Telecom Company and Bayanat al-Oula for Network Services. These ISPs must follow the same protocols as the state-run service (e.g., filtering content).[7]

Since the Internet became widely available to the public in 1999 and the demand for Internet services started to increase, especially from the commercial sector, the number of Internet users in Saudi Arabia rapidly expanded (from 100,000 in 1999 to one million in 2001, and to more than 16.5 million by the end of 2016). In 2016, nearly all colleges and universities in the country offered free Internet access to faculty and students. Hospitals, banks, and companies within the country also used the Internet to provide citizen-facing services. More recently, the Saudi government placed increased emphasis on Internet uptake as a catalyst for economic growth, more efficient government operations, and increased access to education and public services. The government also viewed this as a means to diversify from an oil-dependent economy.

Today, Saudi Arabia connects 21 million or nearly 70 percent of its population to the Internet. While other Gulf countries like the United Arab Emirates, Qatar, and Kuwait have higher penetration rates, the Saudi population is embracing the opportunities associated with the Internet and setting the example for the rest of the Arab states.[8] In addition, the Saudi people are among the most active social media users in the world – and largest adopters of Twitter in the Arab region. Moreover, their high rate of mobile phone ownership (177 percent market penetration) is driving up Internet usage and increasing the demand of mobile broadband services. Finally, a large number of the population is increasingly turning to circumvention tools, such as Hotspot Shield, to access banned content and services.

Saudi Arabia has the largest ICT market in the Middle East by both capital volume and spending, and this market is quickly becoming one of the most coveted by local and international companies. In fact, while the Saudi IT industry currently contributes only to a modest 0.4 percent of the country's gross domestic product (GDP) and the Kingdom's ICT market continues to be import-driven – with over 80 percent of ICT expenditure by foreign companies[9] – the IT sector is considered one of the fastest growing industries, offering massive development opportunities. The cyber security market alone is expected to reach more than $3.4 billion by 2019.[10]

The highly profitable STC, now a publicly traded company, is still the dominant ISP in the country and among the largest operators in the Middle East, offering the majority of mobile, landline, Internet, and television services in Saudi Arabia.[11] However, the company lost its monopoly on mobile and Internet services when other ISPs, such as Mobily and Zain, entered the market place in the mid to late 2000s. In 2008, STC began implementing 3G technology, allowing for increased digital communications as well as greater reliability and speed. That same year, Zain entered the

Saudi Arabian mobile market with 4G Long Term Evolution (LTE) services.

Despite the 70 percent Internet penetration and expanded mobile use, e-commerce is still under developed. There are at least three contributing factors to this delay. First, it is difficult to start a new business in the Kingdom. Second, ICT costs are still high (Saudi Arabia ranks 101st in the world for ICT affordability[12]), and businesses often prefer to avoid the costly investments required to embed ICTs into their business operations. Third, the oil economy still dominates the economy, representing more than 90 percent of government revenues, with companies largely focusing on the extraction, refinement, and distribution of oil and liquid natural gas (LNG).

The Saudi government recognizes that to improve the country's economic strength, it must diversify its reliance on oil. As such, Crown Prince Muhammad bin Salman – next in line to the throne after King Salman bin Abdulaziz Al-Saud – has laid out his vision to revolutionize the Saudi economy by ending its dependency on oil and building a "strong, thriving, and stable Saudi Arabia that provides opportunities for all," and that is never "at the mercy of commodity price volatility or external markets."[13] This vision was set forth in the 2016 "Saudi Arabia Vision 2030," an economic reform agenda that provides the country with a roadmap of goals and objectives for the future improvement of Saudi Arabia.[14]

Although this ambitious economic and development strategy includes digital development as one of its objectives, it is not the primary focus. However, the plan does recognize that in order to fully realize the economic benefits of ICT, it must also facilitate the access to and use of technologies such as cloud computing, and expand the variety of Internet-facing services provided to citizens. The plan rests on three main pillars: (1) Saudi Arabia's position as the heart of the Arab and Islamic worlds; (2) its role as an investment powerhouse; and (3) its strategic location as the hub connecting Asia, Europe, and Africa.[15] This plan, like many other past efforts to move the Saudi economy away from its reliance on oil production, tries to balance religious conservativism with modernization. This creates tension regarding how modern technology and the Internet should be appropriately used and harnessed to enhance the economic wellbeing of the Kingdom.[16]

Vision 2030 is aligned with the priorities already highlighted in the National Transformation Plan (NTP) 2020, and underscores the importance of increasing the private sector's role by diversifying into service sectors such as healthcare, education, infrastructure construction, recreation, and tourism. Other goals of Vision 2030 include: boosting foreign direct investments; reducing the role of the public sector and bureaucracy while empowering the private sector to become the main employer; creating better job opportunities and developing relevant skills in the workforce; provisioning outstanding healthcare; and enhancing government spending on military manufacturing equipment and ammunitions.

The Saudi Council of Economic and Development Affairs has been tasked with setting up the necessary mechanisms and measures to implement this vision, coordinate efforts among all relevant stakeholders, and monitor progress. The Council established a number of bodies, including a National Center for Per-

formance Measurement, a Delivery Unit, and a Project Management Office, to initiate, manage, monitor, and evaluate the various current proposals as well as future programs.

Although Saudi Arabia's Vision 2030 promises to open up many economic opportunities for investors and move the country toward radical transition, the ambitious economic plan does not address political or social reforms, and does not account for the requisite additional foreign skilled labor. It is also unclear whether the Vision 2030 accounts for the country's ability to generate the sustained revenues to fund the infrastructure development needed for the new service-enabled economy.[17] The persistent decline in oil prices is already curtailing revenue generation required to implement the proposed changes.

Moreover, the Kingdom remains afflicted by complex and dynamic security challenges that have led to increased regional instability.[18] These challenges include costly military operations in Yemen and Syria, increasing violent extremism from the Islamic State of Iraq and Levant (ISIL) and other extremist groups, mounting tensions with Iran, and an ongoing diplomatic crisis with Qatar. The government's intentions to attract foreign direct investments and increased participation by private sector companies in their economy may also be jeopardized by the increasing number of cyber attacks against critical infrastructures and private corporations.

In August 2012, Saudi Arabia's state-run oil company Saudi Aramco suffered a serious and destructive cyber attack. The Shamoon malicious software corrupted tens of thousands of hard drives, shut down employee email, destroyed data, and damaged almost three-quarters (or 75 percent) of the company's IT infrastructure assets.[19] It took the company weeks to fully restore its business operations. This was seen as a direct attack against the Kingdom since Saudi Aramco is a state-owned enterprise and represents over 80 percent of the government's revenues. It is also the world's largest oil producer and represents over 10 percent of the global oil supply and at least 25 percent of the supply of LNG. The malware was intended to migrate from the business systems into the oil and gas production and distribution networks. Even a partial disruption of the oil production facilities could have had an immediate impact on oil supplies and prices and subsequently, on the global economy. This event raised awareness across the entire Saudi government regarding cyber threats and renewed its concerns about the country's resilience to future cyber attacks.[20]

Following the 2012 Saudi Aramco incident, the Saudi government started investing significant resources toward advancing its cyber security capabilities and implementing both domestic and international measures to address its cyber *insecurity*. Domestically, Saudi Arabia began developing a "National Information Security Strategy (NISS)" – a first attempt at creating a national framework for cyber security, risk mitigation, and resilience, which focuses on people, processes, and technology.[21] The draft document recognizes the "complexity of today's interconnected computer networks [and] the rapidly growing dependence of economic and financial activity on ICTs," and tries to provide "an integrated strategy designed to meet the Kingdom's national information and ICT security objectives," while also supporting the Kingdom's long-term national econom-

The draft National Information Security Strategy and Vision 2030 stress the need for Saudi Arabia to advance the overall security and resilience of the country and "provide an effective and secure foundation for the Kingdom's evolution to a knowledge-based economy."

ic vision and strategic plans.[22] Both the NISS and the national economic agenda – Vision 2030 – stress the need for Saudi Arabia to advance the overall security and resilience of the country and "provide an effective and secure foundation for the Kingdom's evolution to a knowledge-based economy."

However, the NISS is mainly focused on creating a centrally-managed information security environment along with the necessary policies, regulations, and a skilled workforce, and it leaves out other critical aspects of national cyber security and Critical Infrastructure Protection (CIP). The NISS calls for the development of separate strategies for cyber security and CIP as "outside the scope of NISS" but as "important complements to the NISS and necessary for comprehensive protection of the Kingdom's vital national interests and assets."[23] It also warns that the effective implementation of such strategies will require the Kingdom's top leadership consensus, and recognizes that one of the main challenges will be convincing government agencies to unanimously agree on a centralized national information security environment.

Despite the draft NISS strategy, the majority of security institutions and ministries in the country have developed their own rules and infrastructures, and operate their own security systems and measures with little to no central coordination. These separate and isolated efforts are further compounded by the lack of a clear, competent authority responsible for the overall cyber security of the nation.

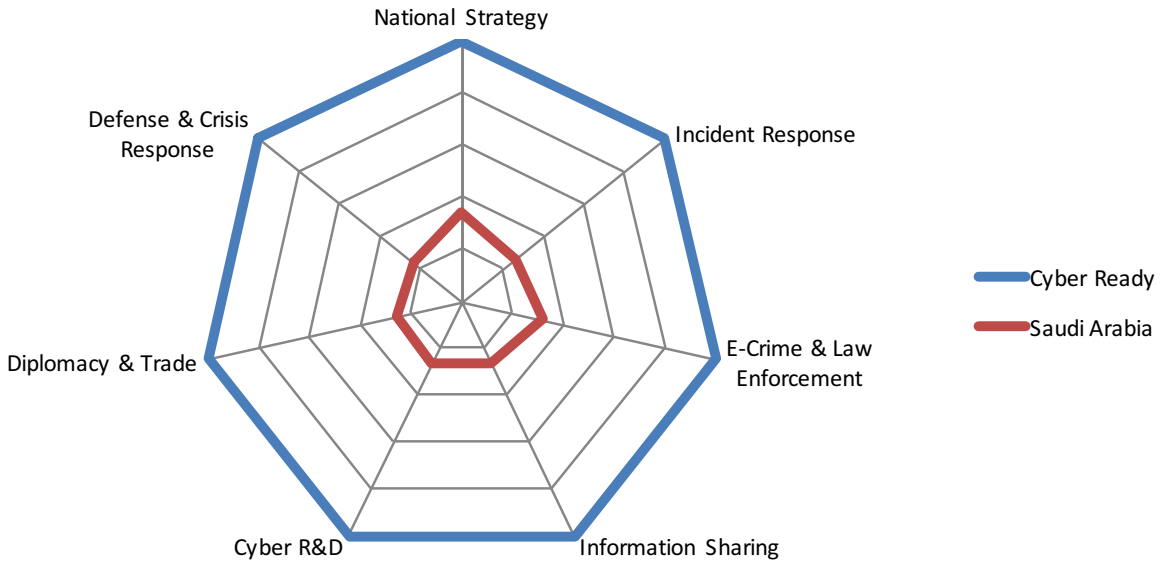
Yet, in July 2017, King Salman issued a series of royal decrees that most notably established a Presidency of State Security – a new state security agency responsible for counter-terrorism and domestic intelligence efforts. This agency will include departments that were formerly part of the Ministry of Interior (MoI), such as special emergency forces, technical affairs, security aviation, civil and military personnel, and other divisions responsible for fighting terrorism and addressing other security issues. The decrees directed also that the National Cyber Security Center (NCSC) be repositioned from the MoI to the Presidency, perhaps as early as January 2018. The NCSC will become the focal point for cyber security in the Kingdom. Finally, the string of decrees ordered changes in positions for senior personnel of the elite royal

In July 2017, King Salman issued a series of royal decrees that established a Presidency of State Security, repositioning the National Cyber Security Center under the Presidency to become the focal point for cyber security in the Kingdom.

guard and the MoI, and elevated the head of the newly-created Presidency of State Security, Abdulaziz bin Mohammed al-Howairini, and his deputy to the rank of ministers. The moves are aimed at centralizing authority in security matters, including cyber security, counter-terrorism, and domestic intelligence, and positioning them under the authority of a single body, which will respond directly to the King and Crown Prince.[24]

As the Kingdom stands up this new organization and reorganizes its leadership and initiatives in the coming months, it must address the fragmented nature of the country's cyber security responsibilities that have contributed to its lack of strategic cyber security planning so far, as well as ensuring that it invests its limited amount of resources to identify immediate and long-term cyber threats to improve the country's overall cyber security posture.[25] Understanding the risks and opportunities afforded by ICT innovations while at the same time tempering its approach to filtering online content will be essential components on the path toward achieving the ambitious goals set forth in its Vision 2030 strategy and reaping the benefits associated with being part of the global Internet economy.

The Cyber Readiness Index (CRI) 2.0 has been employed to evaluate Saudi Arabia's current preparedness levels for cyber risks. This analysis provides an actionable blueprint for Saudi Arabia to better understand its Internet-infrastructure dependencies and vulnerabilities and assess its commitment and maturity to closing the gap between its current cyber security posture and the national cyber capabilities needed to support its digital future. A full assessment of the country's cyber security-related efforts and capabilities based on the seven essential elements of the CRI 2.0 (national strategy, incident response, e-crime and law enforcement, information sharing, investment in R&D, diplomacy and trade, and defense and crisis response) follows:



Kingdom of Saudi Arabia Cyber Readiness Assessment (2017).

1. NATIONAL STRATEGY

In 2011, the Ministry of Communications and Information Technology (MCIT) – one of the government agencies responsible for cyber security and digitization of government services in Saudi Arabia – began developing the country's first "National Information Security Strategy (NISS)." [26] The 90-page draft, developed and produced by a group of international senior consultants and national experts, is currently in its seventh iteration.

The Saudi Ministry of Communications and Information Technology (MCIT) drafted the first National Information Security Strategy in 2011.

The need to articulate a national cyber security strategy emerged from the recognition that the Kingdom faces growing, diverse threats to its national security, economic wellbeing, and cultural values. According to the NISS, "national and international interconnectivity creates significant new vulnerabilities and presents new types of threats to the Kingdom's economic and cultural activities. These new threats could in some cases shutdown, corrupt or even destroy critical information and communications technologies (ICT) systems."[27] Such threats include the possibility that an adversary might "seize control and use an ICT system to directly harm or go against the Kingdom's interests."[28]

The strategy articulates a clear vision for Saudi Arabia, stating that its goals are to provide a secure and robust digital environment that incorporates best practices from around the world and that relies on highly qualified Saudi experts and practitioners. The draft strategy has five main goals, namely: (1) developing a secure, reliable, and resilient information infrastructure; (2) training a professional cyber security workforce; (3) creating an information security environment that inspires trust and confidence through transparency and cooperation; (4) supporting e-government services and infrastructures that meet the Kingdom's security objectives and ICT plans and strategies; and (5) promoting economic growth through research and development as well as entrepreneurial efforts. Further, the NISS is built around ten general objectives that encompass and support the five broad goals stated above, including: (1) developing appropriate and consistent information security policies, directives, guidance, and practices; (2) enhancing the security, reliability, availability, and resilience of the Kingdom's information systems and ICT infrastructure; (3) improving human resources; (4) establishing information security threat analysis and mitigation capability; (5) reducing and preventing ongoing ICT exploitation; (6) implementing information security compliance and tracking processes; (7) fostering research, innovation, and entrepreneurship; (8) ensuring adequate information security protection of essential ICT infrastructure and systems; (9) promoting national and international cooperation and information sharing; and (10) increasing awareness of security risks and individual responsibilities.[29] However, despite these broad goals and general objectives, the document is still aspirational and does not offer a clear implementation plan or specific guidelines to achieve the desired goals.

The draft NISS recognizes that its vision is far from being realized. For instance, there is currently no uniform set of cyber security policies and standards, and individual organizations and ministries have generally developed their own approaches to cyber security and set up their own security environment with little commonality. Similarly, risk and threat assessments are lacking in standards, which makes it difficult for government organizations to compare perceived threats in a coherent manner consistent with developing effective strategies and policies. There is also a lack of sophisticated and comprehensive disaster recovery planning procedures that incorporate cyber security. In addition, the draft strategy does not clarify the Saudi cyber security national architecture and does not identify a competent authority responsible and accountable for the overall cyber security posture of the country. Finally, the biggest challenge to closing the gap between where the Kingdom's cyber security posture currently is and where the NISS envisions it to be, is the lack of a sufficiently skilled and qualified cyber security workforce – the country currently has a shortage of over 50,000 ICT specialists according to the Minister of Communications and Information Technology, Abdullah Al-Swaha.[30]

In order to address these shortcomings, the draft NISS includes numerous recommendations including the creation of a centrally-managed organizational structure by 2020 – a National Information Security Environment (NISE) – that incorporates all relevant stakeholders in the country and that will be "responsible for the detailed implementation of the NISS objectives and initiatives," and the establishment of a national risk assessment framework to support an effective and secure information security environment.[31] However, it is unclear what the NISE organization will look like, what its positional authority will be, and what other cyber security responsibilities will be assigned to existing, combined, or new organizations in the country. The draft strategy states that "the appropriate authority in the Kingdom shall decide which entities and sub-entities to establish, [and that] the specific roles for existing government agencies concerned with information security [still] need to be determined."[32] In July 2017, King Salman issued a series of royal decrees establishing a Presidency of State Security – a new state security agency responsible for counter-terrorism, domestic intelligence efforts and cyber security. The Presidency will position these responsibilities into a single body reporting directly to the King and Crown Prince.[33] It is unclear whether the draft NISS will change and these recommendations reprioritized. Nonetheless, currently Saudi Arabia does not have a published cyber security strategy or policy.

In 2013, a royal decree established the National Centre for Electronic Security (NCES) under the MoI. The NCES was later renamed the National Cyber Security Center (NCSC), and the 2017 royal decrees elevated it and repositioned it under the Presidency of State Security, which may also become responsible for the next iteration and formalization of the NISS. In addition, the royal decrees established that the NCSC will become the focal point for cyber security in the Kingdom, perhaps as early as January 2018. Currently, the responsibilities for cyber security in Saudi Arabia are shared among the MCIT, the MoI, and other government ministries and agencies. NCSC acts like a government computer emergency response team (CERT) and is charged

with protecting the Saudi government and Critical National Infrastructure (CNI) operators' information and communication systems and networks.[34] The NCSC operates out of Riyadh and is tasked with a number of responsibilities including: devising national standards, rules, and regulations to protect the country's information infrastructure and critical assets; identifying risks and producing threat intelligence; coordinating efforts to respond and recover from cyber incidents at the national level; and facilitating the flow of information and security warnings between different sectors. For example, the NCSC has developed recognized expertise in information assurance and end-to-end cyber defense capability, with both analytics and forensics components, and shares threat intelligence with government agencies and a number of CNIs in the Kingdom. Some of these missions, however, are still maturing and at different stages of operational effectiveness.

The financial commitments are unclear for each of the proposed initiatives within the NISS. The national budget, negotiated bilaterally between the Ministry of Finance and the Saudi government's various line agencies, is not subjected to legislative review and, therefore, is not publicly available. Estimated spending for different sectors are available, but they do not contain a detailed breakdown of cyber security expenditures.

Despite some notable progress in increased cyber security awareness and capability, there is still a substantial gap in terms of national-level preparedness for cyber risks between Saudi Arabia and comparable developed countries. While Saudi Arabia has put forward several cyber security-related initiatives and intends to invest in innovative cyber security technologies, the country still lacks an overall cyber security strategy, a set of common cyber security policies and standards, and a consistent national architecture for cyber security. In upcoming months, the Presidency of State Security will have an opportunity to set Saudi Arabia on a path toward becoming more cyber ready by developing and formalizing a national cyber security framework and strategy.

2. INCIDENT RESPONSE

In 2016, Saudi Arabia experienced a new wave of cyber attacks that affected government agencies and private sector companies, and placed renewed urgency on the need for the country to develop cyber security capacity and resilience. These attacks used a malicious software similar to the one in the 2012 Saudi Aramco attack and caused widespread disruption of critical infrastructures by rendering them inoperable.[35] During the 2nd Annual International Cyber Security Conference held in Riyadh in February 2017, the Director General of the Saudi National Cyber Security Center (NCSC), Saleh Ibrahim Al-Motairi, stated that the Kingdom had sustained almost 1,000 cyber security attacks targeting critical infrastructure, seeking to steal data, and causing services interruption, in 2016 alone.[36]

Cyber incidents of national interest like these fall under the responsibility of the Saudi Computer Emergency Response Team (CERT-SA), which was established in 2006 to serve as "the trusted authoritative reference for information security."[37] In 2007, CERT-SA started providing incident handling consultancy services, in addition to detection, prevention, awareness raising, educational, and training functions. Overall, the CERT-SA offers multiple services, including: (1) helping organizations contain and manage security threats and, if asked, respond to national-level cyber incidents; (2) promoting cyber security awareness through online resources and ongoing awareness campaigns and seminars; (3) offering education and training activities, including working with universities to develop customized training courses for government agencies and businesses; (4) publishing threat warnings, intrusion alerts, and advisories; (5) assisting stakeholders in developing and implementing their own security procedures and processes; and (6) providing feedback and information on how to handle specific cyber security-related issues.[38] In addition, CERT-SA collects information about specific events and response efforts, and conducts post-event analysis and reporting. If asked, CERT-SA will analyze and then develop prevention and detections solutions to cyber incidents. It may also try to quantify the extent/cost of the damage caused by a cyber incident.[39]

In 2006, Saudi Arabia established its first Computer Emergency Response Team (CERT-SA) to serve as the trusted authoritative reference for information security.

Although CERT-SA provides incident response support and additional services, it is not seen as the central authority responsible for whole-of-government and whole-of-society incident response coordination and has yet to develop an incident response plan for emergencies and crisis. CERT-SA is still largely perceived as a reactive organization, mostly focused on providing press releases, advisories, and information on current threats, and offering *ad hoc* incident response support. At this time, they have not developed the capability for coordinated responses to full-scale cyber attacks and dissemination of timely and actionable information. The 2012 Saudi Aramco attacks led to renewed emphasis on the role of national computer emergency response teams, such as CERT-SA, in responding to and mitigating the effects of cyber incidents of national interest. After that damaging cyber attack, CERT-SA increased its efforts to disseminate relevant information to detect and prevent cyber attacks, but there is still not a coordinated effort to develop mechanisms to effectively and expeditiously share threat intelligence and situational awareness with government agencies and organizations in order to prevent and mitigate cyber threats.

Moreover, there have been planning efforts to establish a formal threat intelligence sharing platform under the NCSC, which would support the security of CNIs and government entities, as well as provide additional proactive and reactive services, such as: cyber incident

response planning, supervision, and consultation; malware analysis; compromise assessments; and cyber incident remediation.[40] However, this platform has yet to be fielded.

In addition, the draft NISS calls for the establishment of a "national Security Operations Center (SOC), which would collect and disseminate threat and intelligence information, analyze attacks, recommend mitigation actions, coordinate a national response [and serve] as a resource to assist decision makers in understanding the impacts of ICT exploitation and deciding how best to address and reduce [cyber] risks."[41] However, the NISS does not specify whether the SOC would replace, support, or work alongside CERT-SA and the NCSC to share more immediate or urgent threat information. NISS only mentions that the national SOC would sit under the new National Information Security Environment (NISE) organization to support Saudi national-level crisis management efforts, and "would work with existing centers and capabilities to facilitate national information sharing and coordinate mitigation and incident response actions."[42] The new Presidency of State Security will need to clarify the roles and responsibilities of each of these centers in order to maximize resources and increase their overall effectiveness.

In an effort to begin assessing national-level cyber risks and developing a consistent national cyber risk assessment and management process, the NISS calls for the creation of a dedicated National Risk Assessment Function (NRAF) under NISE, which in turn would "help implement a national Risk Process Management System that provides a common risk framework for the Kingdom."[43] Currently, neither the processes nor organizations exist and the entities in Saudi Arabia use different criteria to evaluate risks and assess their level of seriousness/urgency. The NISS recognizes that the problem is two fold. First, in the current approach, senior management "must evaluate and make high-level risk mitigating decisions on issues that cut across traditional ministry or organization boundaries," but they lack "a common risk assessment framework to enable them to make informed decisions involving risk in the context of current and future priorities, finite resources, and global complexity."[44] Second, the various ministries have a tendency to work separately in their respective mission areas and have not yet recognized their digital dependency and need for common practices in cyber security. To address these problems, the NRAF would establish "selected, risk-educated, and trained senior Saudi executives," and would "have the authority to oversee security risk assessment of various national integrated information infrastructures (N3i) within the Kingdom."[45] However, this organization has not been established and the NISS strategy recognizes that the biggest challenge to its effectiveness will be getting N3i senior management to collaborate on risk assessments and management functions, since the fear of exposures of organizational weaknesses and lack of trust among key stakeholders still hampers effective collaboration.

In the absence of more formal mechanisms for threat monitoring and analysis and in response to an increase demand for cyber security products, foreign private firms have started providing cyber security services, including threat monitoring and data management services, in both the government and commercial sectors. This has attracted many multinational IT and security companies to the Saudi market, with some of them forming innovative partnerships with local IT and telecommunications firms. For

*Proposed NISS Risk Assessment and Management Cycle. **

example, a foreign-Saudi partnership between IBM and Saudi Arabian mobile operator Mobily established a global SOC in Riyadh, which uses IBM security services infrastructure to assist analysts in collecting, analyzing, correlating, and prioritizing security logs and events. In 2014, this global SOC was selected by the Saudi Ministry of Education to help strengthen its cyber security posture by conducting real-time analysis, creating an early warning system for potential threats, and protecting the ministry data from foreign third-party access.[46]

The MCIT recognizes the need to conduct regular national-level cyber security exercises that test response, recovery, and restoration plans, but it is unclear whether those exercises are consistently taking place, if at all.[47] The only type of cyber security exercise reported occurred during the 2014 Saudi military exercises dubbed "Sword of Abdullah," which included training on electronic warfare.[48]

Despite all of these initiatives, the Saudi approach to incident response remains largely reactive. Recent attacks have sparked renewed interest in accelerating planned initiatives toward becoming more proactive and resilient to cyber incidents.

3. E-CRIME AND LAW ENFORCEMENT

Saudi Arabia is a signatory of the "Arab Convention on Combating Information Technology Offenses" (commonly known as the Arab Convention).[49] This international legal framework among the League of Arab States was enacted in 2010 with the aim of enhancing cooperation between the Arab countries "to combat information technology offences threatening their security, interests, and the safety of their communities," and enabling parties to "adopt a common criminal policy aimed at protecting the Arab society again information technolo-

** Image adapted from the draft National Information Security Strategy, produced by the Saudi Ministry of Communications and Information Technology, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/SaudiArabia_NISS_Draft_7_EN.pdf.*

Saudi Arabia is one of the 18 members to sign the Arab Convention on Combating Information Technology Offences, but it has yet to ratify it.

gy offences."[50] Saudi Arabia is one of the 18 member states to sign the Arab Convention, but is the only country that has not yet ratified it. Moreover, the convention is quite vague in its definitions and provisions to combat cyber crime and, despite its wide acceptance, it has not been formally activated. In fact, there is no reference to its provisions in any of the Arab nations' cyber crime laws, and coordination between the 18 state parties remains ineffective.[51]

In addition, Saudi Arabia is not a party to nor is in the process of joining any of the global anti-cyber crime agreements, like the Council of Europe's "Convention on Cybercrime" (commonly known as the Budapest Convention) or the Shanghai Cooperation Organisation's (SCO) "Agreement on Cooperation in the Field on Ensuring International Information Security."

Saudi Arabia does participate in some international dialogues and strategic partnerships to increase cooperation on cyber crime. It has developed bilateral relationships and informal channels such as police-to-police and agency-to-agency cooperation, and is committed to further expanding international collaboration on international standards development, global ICT security policy, and cyber crime initiatives and research.[52]

Domestically, Shari'a law is the official basis of criminal justice in Saudi Arabia. Saudi Arabia has enacted two major cyber-related laws – the Electronic Transaction Act and the Anti-Cyber Crime Law. Together these laws address cyber crime and cyber security issues, while also attempting to encourage and regulate the use of e-commerce and other Internet-facing services.

The 2007 Electronic Transaction Act regulates e-commerce and establishes a legal regime for electronic transactions and digital signatures in Saudi Arabia.[53] This Act consolidates the use of electronic transactions in the public and private sectors, at local and international levels, and advocates their use in commerce, medicine, education, e-government, e-payment systems, and other applications. In addition, the law seeks to protect digital records, and limit and prevent potential abuse, fraud, and embezzlement. It recognizes the equal validity of transactions carried out online and those carried out in a physical space, and regards the legal equivalence of electronic signatures and written signatures.

The Communications and Information Technology Commission (CTIC), created under the Act, is responsible for the implementation of the law, including issuing licenses to authentication services providers (ASPs); verifying compliance by ASPs; and guaranteeing continuity of services and suspending or canceling licenses. The MoI and MCIT are jointly responsible for issuing general policies and developing plans and programs for electronic transactions and signatures. The MoI established the National Information Centre (NIC) to provide services for exchanging and storing information on a matrix of interconnected branches

throughout Saudi Arabia, offering operations in the regions and supporting the Hajj (i.e., the pilgrimage to Mecca). Moreover, the Act mandated the creation of a National Center for Digital Certification (NCDC), which provides an integrated system for managing the Public Key Infrastructure (PKI) that enables Internet users to perform secure e-transactions. In association with the Ministry of Finance, the NCDC operates the Saudi Electronic Data Interchange (Saudi EDI) project to facilitate quick and transparent business transactions.[54] While the Act was originally perceived as a way to improve the environment for e-commerce – import and export electronic transactions – much of its emphasis so far has been on government transactions, and the law has not been updated in over ten years. There is now increased pressure to update the law to keep pace with the changing economic and technological environment and international standards.[55]

In 2007, the Anti-Cyber Crime Law (ACCL) was passed. It had four primary objectives: (1) maintaining data security; (2) increasing IT employment; (3) providing protection for intellectual property across networks; and (4) protecting the public interest and morals.[56] While this law is designed to protect users from cyber crimes, it also contains clauses that limit freedom of expression. For example, the ACCL criminalizes "producing something that harms public order, religious values, public morals, the sanctity of private life, or authoring, sending, or storing it via an information network." It also imposes penalties, including up to ten years in prison and fines up to five million riyals (~$1.3 million) depending on the severity of violation or crime committed. Additional penalties can be added if the crime is part of an organized crime syndicate, if the violator is a public official and the crime is related to public influence, if minors are involved, or if it is a repeated offense.[57]

In addition, the ACCL provides a legal framework to prosecute cyber crimes such as theft of sensitive data and cyber disruption, but it does not address prevention, detection or collaboration either inside the Kingdom or with international partners, thus making prosecution of cross-sector and cross-border crimes particularly difficult. In the case of the 2012 Saudi Aramco attack, for example, the ACCL would have been extremely hard, if not impossible, to apply since the threat actor was believed to be a proxy of the Iranian government. Moreover, there is still a lack of sufficiently trained court judges, prosecutors, lawyers, and law enforcement officials to address different elements of cyber crime and successfully investigate and prosecute offenders.

Moreover, the ACCL has triggered widespread criticism by legal experts and human right activists for what is being perceived as an overly zealous use of the "moral" violations to fine, arrest, or prosecute activists, bloggers, and Saudi citizens for political or religious purposes, rather than using the law to prosecute actual cyber crimes and protect digital assets. For example, in 2015, a 32-year old Saudi woman was sentenced to jail for two months and fined more than $5,000 for using WhatsApp to, in the opinion of the court, defame another Saudi citizen. In 2016 – as punishment for defaming the Ministry of Health on Twitter – one physician was sentenced to 6 months in prison and a pharmacist received 4 months in prison.[58] In 2016, changes were made to the ACCL giving officials greater latitude not to prosecute cyber crimes that cause damage to networks, but to publicly name offenders after final rulings have

been issued in cases involving religious values and public morals. These changes are diverting attention and resources away from cyber crimes and may negatively affect the country's ability to attract foreign direct investment and consequently, its ability to diversify from an oil-based economy.[59]

Internet use is persistently monitored by the CITC, which employs strict filtering on online content and social media posts considered "harmful," "illegal," "anti-Islamic," or "offensive," and consistently blocks websites related to pornography, gambling, drugs, extremist ideology, as well as pages belonging to human rights or political organizations.[60] Saudi Arabia publicly acknowledges censoring morally inappropriate and religiously sensitive material, consistent with Shari'a law. Yet, in recent years law enforcement agencies expanded inspection and interception by breaking or bypassing encryption to inspect political, social, and religious content on websites, blogs, chat rooms, social media sites, emails, and phone text messages in the name of protecting national security and maintaining social order.[61]

Moreover, the Ministry of Culture and Information requires that blogs, forums, chat rooms, and other popular sites obtain a license from the ministry to operate, while CITC requires mobile network operators to register subscribers' real names, identity numbers, and now even their fingerprints in order to "limit the negative effects and violations in the use of communication services."[62] Users have become particularly careful about what they post, share, or "like" especially after the passage of the 2014 Anti-Terrorism Law, which defines terrorism in such vague terms as "insulting the reputation of the state," "harming public order," or "shaking the security of the state."[63] The Anti-Terrorism Law effectively criminalizes all content questioning Islamic religious doctrine or expressing support for any type of "banned groups" or political reforms.[64]

Aside from the aforementioned laws and a general right to privacy contained in the Basic Law of Governance, there are few privacy protection regulations associated with personal privacy and personal data. For example, a national data protection regulator does not exist. Furthermore, there is no formal customer notification or registration requirement before the government or a company can collect or process data. The lack of data governance processes or regulations leaves data transfer and data residency requirements ambiguous. There is no clear definition of "personal data," and no requirement to notify data security breaches to any individual or entity in Saudi Arabia.[65]

Finally, the draft NISS strategy does not include any mention of human or financial resources allocated to support additional legal and policy initiatives to protect society against cyber crime, to reduce criminal activity emanating from the country, or to promote coordination mechanisms to address international and national cyber crime. The draft NISS strategy does not clarify how it plans to expand law enforcement capacity. As Internet use becomes more widespread and as more connected devices become avenues for infection and exploitation, Saudi Arabia will need to increase the capacity of its law enforcement agencies and commit resources to effectively respond to increased cyber crime and reduce infrastructure weaknesses.

4. INFORMATION SHARING

While Saudi Arabia does not have a national information sharing policy, the draft NISS strategy highlights the importance of national and international information sharing and cooperation, and is committed to expanding information exchanges on emerging threats and vulnerabilities, and appropriate mitigation technologies.

The NCSC shares threat intelligence with government agencies, a number of CNIs, and other interested stakeholders in the Kingdom, but this capability is still maturing. There have been planning efforts to establish stronger information sharing mechanisms, including a threat intelligence sharing platform under the NCSC that would further support the security of the CNIs as well as government entities. Early warning of threats and malicious activities occurring in CNIs or other parts of the world are important and necessary components of a strong national cyber security posture. For example, the May and June 2017, cyber incidents that exploited vulnerabilities in Microsoft's software sparked global information sharing and threat response activities. As one nation or industry became victim of those cyber incidents, others were able to quickly learn from the events, shut off vulnerable components of their networked infrastructures, and communicate the software patches needed to protect their infrastructures and enterprises.[66] Indeed, the NISS strategy emphasizes that "the equation is simple. As cooperation, collaboration, and information sharing (both within the country and across borders) increases, the risk of information loss and ICT systems exploitation decreases."[67]

While Saudi Arabia does not have a national information sharing policy, the draft "National Information Security Strategy" does highlight the importance of information sharing and cooperation as a key strategic area.

Nonetheless, Saudi Arabia does not have a strong tradition of sharing information internally, let alone with international agencies. Rivalries and jealousy among ministries guarding their own bureaucratic institutions and missions, compounded by the rapid rise of technology, have made it difficult for a single strategy to take hold effectively with regard to sharing cyber security information. The Kingdom has also been reluctant to share information on an international level; while it shares economic interests with other countries in the region, military tensions and competing political interests have hindered the free flow of information across borders. The establishment of the Gulf Cooperation Council (GCC), which includes Saudi Arabia, the United Arab Emirates, Bahrain, Kuwait, Qatar, and Oman, may be a venue by which greater trust and increased information sharing could be explored.[68]

Saudi Arabia is also a member of the Organisation of Islamic Conference-Computer Emergency Response Team (OIC-CERT), a group of 18 countries, including Egypt, Iran,

Turkey, and Nigeria, as well as Saudi Arabia. This group includes national CERTs from the various countries and is intended to facilitate information sharing among Islamic countries. The OIC-CERT organizes training, workshops, and exercises designed to provide real-time experience in addressing cyber threats and crises, including timely and actionable information sharing.[69]

The NISS recognizes that the Kingdom requires much progress in this area. The NCSC and the new Presidency of State Security now have an opportunity to enhance and expand the exchange of actionable information both inside and outside the government. Each ministry, CNI, business, and international partner is in need of information that can improve their security posture. Currently, the only mechanisms used for sharing information within the government and across critical industries are offered by CERT-SA and the NCSC. In the coming months, however, as the government considers standing up a national SOC and formalizes the NCSC's new role, timely and actionable information sharing can become a reality for the country.

5. INVESTMENT IN RESEARCH AND DEVELOPMENT

The draft NISS states a clear intent to create "a flourishing and continuing information security economic sector of research, innovation and entrepreneurial activities," and recognizes the need to "expand research and innovation through international cooperation" in order to help the country develop additional capability in the ICT and cyber security sectors.[70] In particular, the strategy stresses the need to "meet future information security needs by stimulating and directing the Kingdom's information security research and innovation programs that have high potential for commercialization and information security breakthroughs, including cryptographic interoperability, supply chain integrity, computer security, and rapid and effective access control."[71]

The document identifies some initial projects that are designed to expand existing capability, including providing support to researchers and innovators to translate successful ideas and research into patents and commercialized products, but does not clearly state how the government would support, advance, and sustain these efforts. Instead, the strategy proposes the development of a "technology roadmap for research" to guide the country as a whole with input from cyber security communities, other governments and industry from around the world. In addition, it calls for the creation of "a centralized funding advisory capability" to ensure that research and development efforts are aligned with strategic goals and objectives. To this end, the NISS proposes the creation of a Research and Innovation Function that will

Saudi Arabia recognizes that it must develop additional capability in the ICT and cyber security sectors, and has made this a key pillar of its National Information Security Strategy.

oversee grants and funding for specific security programs. This is to be part of the KACST, and will be coordinated with the MCIT.[72]

The draft NISS considers human resources a "key pillar" of its strategy and has proposed several schemes to "expand the capability of Saudi information security practitioners, researchers, innovators and entrepreneurs," and promote cyber security training and awareness.[73] For example, programs have been developed to identify women who are competent in IT and cyber security, and who, with additional training, could quickly meet some of the Kingdom's immediate information security needs. The NISS also suggested that "unemployed young people, who have no formal credentials but have strong computer skills, could be vetted and employed."[74] To respond to this need, the MCIT has launched other talent development programs and partnerships with global IT companies to train over 56,000 Saudi youths on key ICT skills between 2017 and 2020, and has set up a National Information Technology Academy in collaboration with Saudi Aramco to train and develop Saudi talent.[75] Additionally, the NISS proposed a program beginning in primary school that encourages children to acquire computer, analytical, and cyber security skills from an early age, and pairs them with a mentor who supports them through their schooling and into employment.[76] The hope is that these young people will be able to play an important role in maintaining the Kingdom's future security.

While the Saudi government has not developed a formal program or set of incentives, to encourage basic and applied cyber security research at universities and academic institutions, it does support and fund all public universities. Many of these universities offer courses and degree programs on ICT and information security, such as the Masters of Science program in Security and Information Assurance at King Fahd University of Petroleum & Minerals in Dhahran. In addition, the KACST's Communication and Information Technology Research Institute (CITRI) in Riyadh is involved in several research and development projects, spanning from the design of digital and analog integrated circuit chips and integrated electronic systems, to the development of communications and wireless security, robotics and intelligent systems, radar and defense systems, advanced technology for electronic warfare, applied scientific research on lasers and optical fibers, and other prototypes according to the latest international specifications and standards. CITRI plays also a leading role in making KACST the national hub for cyber crime prevention and digital crime forensic research. The Institute provides expertise, consultation, and studies on a variety of topics for government agencies, universities, and companies in order to support their research and technology needs, toward the realization of the national plan objectives for science, technology and innovation.[77] Finally, CERT-SA provides additional technical training, organizes cyber security awareness campaigns, and works with universities, government agencies, and businesses to develop custom training courses and seminars as part of its security quality management function.

Saudi Arabia has the largest ICT market in the Middle East by both capital volume and spending, and, in 2016, it was estimated that the country invested as much as $14 billion in the ICT sector, including cyber security. In addition, there is an increased interest by local and international companies in the Internet

of Things (IoT) enabled by high-speed broadband connectivity, as well as in stronger cyber security measures that facilitate resilience in the wake of potentially damaging cyber threats. Building trust among stakeholders and strengthening confidence in the security efforts undertaken by participants in the online marketplace have been key topics of several workshops and conferences held around the Kingdom, including the most recent IDC CIO Summit of 2016. This conference brought together government officials, Saudi commercial officials, and experts from around the world to explore ICT trends, including cyber security threat solutions for Internet connected and dependent infrastructures.[78]

A significant portion of the $14 billion invested in ICT in Saudi Arabia in 2016 was dedicated to expanding the telecommunication infrastructure – especially high-speed broadband. Today, revenues are largely driven by communications, with an estimated 20 percent coming from increased connectivity. These revenues are expected to rise steadily in this area in coming years. This will require additional infrastructure investments, which may include some security provisions, however, cyber security or resilience is not currently considered a key focus. Both the dominant ISP in the country and one of the largest operators in the Middle East, STC, and competitors Mobily and Zain are investing in connectivity. However, each of these ISPs mainly focus on providing greater access, while data security procedures and processes often take a backseat. Moreover, there is currently little cooperation between these companies.[79]

Private industry and private-public partnerships are starting to collaborate on the launch

Saudi Arabia has the largest ICT market in the Middle East by both capital volume and spending, and, in 2016, it was estimated that the country invested as much as $14 billion in the ICT sector, including cyber security.

of innovation hubs across Saudi Arabia aimed at developing and showcasing technological innovation addressing regional or local economic challenges and promoting economic growth in different sectors. For example, the Saudi Basic Industries Corporation (SABIC) is the principle investor in the Riyadh's Techno Valley innovation hub. This regional innovation hub – the Home of Innovation – is dedicated to technology innovations in the petrochemical and gas industry, and its goals are aligned with the objectives of the Vision 2030 economic strategy of promoting local downstream industry growth, realizing efficiencies for the companies involved, and creating a diverse and sustainable economy for the country. However, cyber security has not typically been addressed in these initiatives as a distinct area of focus.[80]

Following the 2012 Saudi Aramco attack, the Saudi government started to increase its spending for cyber security technology solutions and services, especially in surveillance technology; advanced communication systems; electronic detection equipment; cyber attack detection systems; cyber attack prevention technology;

and biometrics. These areas combine physical security with infrastructure and internal network security strategies. Collaboration with and funding from international partners, including the United States, have received increased interest from the government in recent years.[81] Recently, the Saudi Arabia Military Industries – a state-owned defense enterprise – partnered with United States' defense contractor Raytheon to cooperate on defense-related projects and technology development, including in the area of cyber security. As part of this agreement, the Saudi government will be able to acquire additional cyber security solutions for defense systems and platforms, and Raytheon will establish a new organization (Raytheon Arabia) located in Riyadh and responsible for implementing programs to create indigenous defense, aerospace, security capabilities in the Kingdom.[82] The partnership will therefore contribute to the goals highlighted in the Vision 2030 strategy of developing a Saudi's localized defense ecosystem with expert capabilities and new job opportunities, which will provide a long-term foundation for the country's economic development in this sector.[83]

6. DIPLOMACY AND TRADE

Saudi Arabia does not consider cyber security a top tier foreign policy issue and has not prioritized this area within its Ministry of Foreign Affairs. However, Saudi Arabia is assuming a much more assertive role within the Gulf Cooperation Council (GCC), especially given the increased tensions with Iran and the cyber attacks emanating from Iran's territory. In particular, Saudi Arabia is leading conversations with the GCC to expand cooperation on cyber security and endorse peacetime cyber norms.[84] It is also working with the GCC to establish working groups as part of the May 2015 Camp David accord, in which the GCC agreed to meet at least twice annually to advance partnership on counter-terrorism and streamline the transfer of critical defense capabilities, missile defense, military preparedness, and cyber security.[85]

In addition, Saudi Arabia has been involved in a number of high-level bilateral dialogues with countries like the United States and India aimed at fostering information exchanges related to terrorism financing, money laundering, and the use of cyberspace by terrorist and criminal groups.

Through the NCSC, Saudi Arabia is also promoting regional cyber security cooperation and awareness. As part of these efforts, the Kingdom regularly hosts cyber security-related events such as the annual Cyber Security Forum, which brings together government officials and industry experts from around the Arab world and beyond to explore ways to improve cyber security, enhance threat intelligence capability, and support its Vision 2030 goals.[86] In addition, the Kingdom hosts a government-endorsed annual International Cyber Security Conference, which is attended by the

Saudi Arabia is assuming a much more assertive role within the Gulf Cooperation Council on cyber issues, but has not prioritized cyber security as a top tier foreign policy issue within its Ministry of Foreign Affairs.

highest levels of the MoI, as well as cyber security experts from around the world.[87]

Vision 2030 emphasizes Saudi Arabia's strategic location as the hub connecting Asia, Europe, and Africa. The Presidency of State Security should use its newly established powers and responsibilities to set a vision for the free flow of goods, services, data, and capital across those borders. It should leverage Saudi Arabia's G-20 position and influence to facilitate trusted transactions in the digital economy. Cyber diplomacy is not just about rules of engagement and constraining behaviors. It is also about promoting trade through the free flow of information. Balancing the twin goals of economic prosperity and national security requires a sophisticated diplomatic corps and a commitment to leading the region to realize the Vision 2030 goals.

7. DEFENSE AND CRISIS RESPONSE

Saudi Arabia plays a crucial role in maintaining security and stability in the region due to its economic, political, and cultural importance, as well as its strategic location. Given the complex and dynamic security challenges facing the region – especially the increasing tensions with Iran – the new Crown Prince stated that the Kingdom "will not wait until the battle is in Saudi Arabia but will work so the battle is there in Iran."[88] Moreover, as a result of the cyber attacks Saudi Arabia endured in recent years originating from Iran's territory, cyber security and cyber defense have taken on heightened urgency in Saudi Arabia.

There are several ministries within the Saudi government with cyber security mandates that incorporate cyber defense of the nation, including the Ministry of Defense and Aviation and the Ministry of the Interior. These and other government agencies are beginning to invest in cyber technologies and in advancing their cyber capabilities. In particular, in 2017,

Cyber defense has taken on heightened urgency in Saudi Arabia due to the increased number of destructive cyber attacks the country has endured in recent years.

Saudi Arabia increased its cooperation with the United States through a Security Cooperation Agreement aimed at improving training for special operations and counter-terrorism forces, integrating air and missile defense systems, strengthening cyber defenses, and bolstering maritime security.[89]

In addition, Saudi Arabia seeks to equip other defense forces, including the National Guard, with dedicated cyber capabilities. For instance, the Saudi National Guard is investing nearly half a billion dollars to develop an electronic warfare capability.

There is no evidence that the Kingdom has formalized the military or the intelligence services' cyber security mission in a policy or decree. Moreover, because the Kingdom's budgets are not publicly available, it is difficult to determine the level of funding dedicated to developing cyber capabilities within these institutions. It is

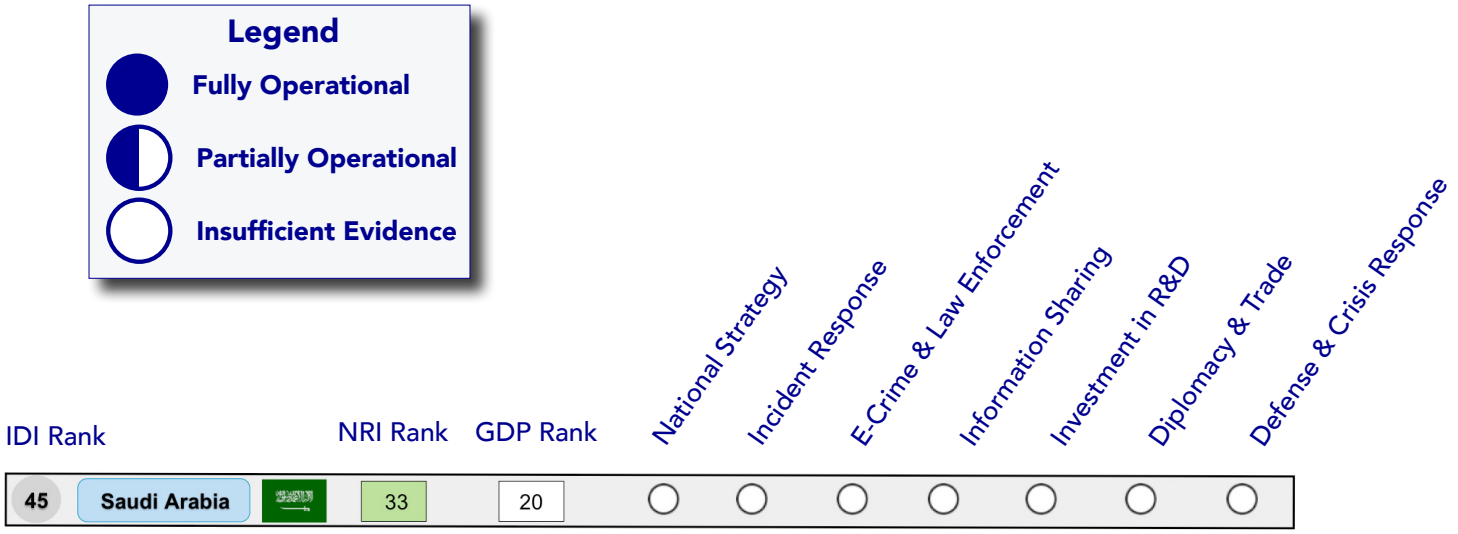
also unclear whether the Ministry of Defense and Aviation is conducting government-wide or military-specific exercises that demonstrate national cyber defense readiness. Nonetheless, Saudi Arabia is at least an active member of the OIC-CERT, which is committed to organizing joint cyber exercises, although it is not clear that any such exercises have actually taken place so far.[90]

CRI 2.0 BOTTOM LINE

According to the CRI 2.0 assessment, Saudi Arabia is still insufficiently prepared in all of the CRI essential elements, although it has made considerable progress in becoming more cyber ready.

The findings in this analysis represent a snapshot in time of a dynamic and changing landscape. As Saudi Arabia continues to develop and update is economic (digital agenda) and national cyber security strategies, policies, and initiatives to reflect a more balanced approach that aligns its national economic visions with its national security priorities, updates to this country profile will reflect those changes and monitor, track, and evaluate substantive and notable improvements.

The CRI 2.0 offers a comprehensive, comparative, experience-based methodology to help national leaders chart a path toward a safer, more resilient digital future in a deeply cybered, competitive, and conflict prone world. For more information regarding the CRI 2.0, please see: *http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.*



ENDNOTES

1. Khalid M. Al-Tawil, "The Internet in Saudi Arabia," *Telecommunications Policy*, vol. 25, issue 8-9, September 2001, 625-632.

2. The Mosaic Group, "The Global Diffusion of the Internet Project – The Internet in the Kingdom of Saudi Arabia," (February 1999): 2, *http://mosaic.unomaha.edu/SaudiArabia_1999.pdf*.

3. Ibid.

4. Hamed A. Alshahrani, "A Brief History of the Internet in Saudi Arabia," *Tech Trends* 60, no. 1, 2016, *https://link.springer.com/article/10.1007/s11528-015-0012-5*.

5. Mahdi Abu-Fatim, "Official on Introduction of Internet Into Kingdom," *Al-Riyadh*, December 6, 1997: 27, as reported in FBIS-NES-97-348, *Daily Report: Near East & South Asia*, December 16, 1997, via *World News Connection*.

6. Communication and Information Technology Commission, *http://www.citc.gov.sa/*.

7. Freedom House, "Freedom on the Net 2016 – Saudi Arabia Country Profile," (2016), *http://freedomhouse.org/report/freedom-net/2016/saudi-arabia*.

8. World Bank, "Internet Users (per 100 people)," 2015, *http://data.worldbank.org/indicator/IT.NET.USER.P2*.

9. Eng. Abdullah Al-Swaha, "ICT Infrastructure Targeted in 1,000 Cyberattacks in 2016," *The Business Year, https://www.thebusinessyear.com/saudi-arabia-2017/eng-abdullah-al-swaha-minister-communications-information-technology/vip-interview*.

10. For more, see: "Saudi Arabia – Telecoms, Mobile and Broadband Statistics and Analyses," Paul Budde Communication Pty Ltd, *https://www.budde.com.au/Research/Saudi-Arabia-Telecoms-Mobile-and-Broadband-Statistics-and-Analyses*.

11. Saudi Telecom Company, "Consolidated Financial Statements for the Year ended December 31, 2016," 2017, *http://www.stc.com.sa/wps/wcm/connect/english/stc/resources/0/7/07a92210-58ff-4466-9a23-f4fc4f14e559/STC+2016+Annual+Consolidated+FS+-English.pdf*.

12. World Economic Forum, "Saudi Arabia," *Networked Readiness Index*, 2016, *http://reports.weforum.org/global-information-technology-report-2016/economies/#economy=SAU*.

13. "Saudi Arabia Vision 2030," *http://vision2030.gov.sa/en*.

14. Ibid.

15. "Full Text of Saudi Arabia's Vision 2030," *Saudi Gazette*, April 26, 2016, *http://saudigazette.com.sa/saudi-arabia/full-text-saudi-arabias-vision-2030/*.

16. Khalid M. Al-Tawil, "The Internet in Saudi Arabia," 625.

17. Hilal Khashan, "Saudi Arabia's Flawed "Vision 2030"," *The Middle East Quarterly*, vol. 24, no.1 (Winter 2017), *http://www.meforum.org/6397/saudi-arabia-flawed-vision-2030*.

18. U.S. Department of State, "Fact Sheet: U.S. Security Cooperation With Saudi Arabia," January 20, 2017, *https://www.state.gov/t/pm/rls/fs/2017/266861.htm*.

19. Melissa Hathaway et al., "Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and An Index," *Potomac Institute for Policy Studies*, November 2015, *http://www.potomacinstitute.org/images/CRIndex2.0.pdf*.

20. Leon Panetta, speech given to Business Executives for National Security, New York, October 12, 2012, *http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136*.

21. Ministry of Communications and Information Technology, "Developing National Information Security Strategy for the Kingdom of Saudi Arabia – NISS, Draft 7," 2013, *https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategy-of-saudi-arabia/at_download/file*.

22. Ibid, 2.

23. Ibid, 2.

24. "Saudi Arabia forms new apparatus of state security," *Arab News*, July 21, 2017, *http://www.arabnews.com/node/1132466/saudi-arabia*.

25. Azhar Unwala, "Cyber security in Saudi Arabia Calls for Clear Strategies," July 27, 2016, *http://globalriskinsights.com/2016/07/cybersecurity-saudi-arabia-calls-clear-strategies/*.

26. Ministry of Communications and Information Technology, "Developing National Information Security Strategy for the Kingdom of Saudi Arabia – NISS, Draft 7," 2013.

27. Ibid, 1.

28. Ibid, 1.

29. Ibid, 2-3.

30. Ibid, 10, and Eng. Abdullah Al-Swaha, "ICT Infrastructure Targeted in 1,000 Cyberattacks in 2016," *The Business Year*.

31. Ibid, 2.

32. Ibid, 20.

33. "Saudi Arabia forms new apparatus of state security," *Arab News*, July 21, 2017, *http://www.arabnews.com/node/1132466/saudi-arabia*.

34. National Cyber Security Center, "About Us," *https://www.moi.gov.sa/wps/portal/ncsc/*.

35. Raphael Satter, "Cyberattacks against Saudi Arabia continue," *Associated Press*, April 26, 2017, and Agence France Press, "Saudi computer systems vulnerable to 'Shamoon 2' virus: telco chief," *Arab News*, January 26, 2017, *http://www.arabnews.com/node/1044566/saudi-arabia*.

36. Aisha Fareed, "Saudi facilities sustained nearly 1,000 cyber attacks in 2016," *Arab News*, March 1, 2017, *http://www.arabnews.com/node/1061151/saudi-arabia*.

37. Suliman Al Samhan, "Saudi Arabia Computer Emergency Response Team," *Communications and Information Technology Commission, https://www.itu.int/ITU-D/cyb/events/2008/doha/docs/alsamhan-national-strategy-CERT-SA-doha-feb-08.pdf*.

38. Computer Emergency Response Team – Saudi Arabia, "CERT-SA

Services," *http://www.cert.gov.sa/index.php?option=com_content&task=view&id=186&Itemid=131*.

39. Ibid.

40. National Cyber Security Center, "Services," *https://www.moi.gov.sa/wps/portal/ncsc/*.

41. Ministry of Communications and Information Technology, "Developing National Information Security Strategy for the Kingdom of Saudi Arabia – NISS, Draft 7," 13, 43.

42. Ibid, 13.

43. Ibid, 13.

44. Ibid, 33-34.

45. Ibid, 35.

46. "Enhancing Saudi Arabia's cybersecurity readiness," *Oxford Business Group*, 2015, *http://www.oxfordbusinessgroup.com/analysis/front-lines-enhancing-kingdom's-cybersecurity-readiness*.

47. Ministry of Communications and Information Technology, "Developing National Information Security Strategy for the Kingdom of Saudi Arabia – NISS, Draft 7," 44.

48. "What Message is Saudi Arabia sending with war games?" *Al-Monitor*, 2014, *http://www.al-monitor.com/pulse/originals/2014/04/saudi-military-maneuvers-sign.html#*.

49. "Arab Convention on Combating Information Technology Offenses," 2010, *http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences*.

50. Ibid.

51. Joyce Hakmeh, "Cybercrime and the Digital Economy in the GCC Countries," *Chatham House*, June 2017.

52. Ministry of Communications and Information Technology, "Developing National Information Security Strategy for the Kingdom of Saudi Arabia – NISS, Draft 7," 5.

53. Kingdom of Saudi Arabia, "Electronic Transactions Law," March 26, 2007, *http://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA_003_%20E_E-Transactions%20Act.pdf*.

54. Ira Piltz, "Internet Law – Saudi Arabia's Electronic Transaction Act," *Internet Business Law Services, http://www.ibls.com/internet_law_news_portal_view.aspx?s=articles&id=BDFDC-5CD-61A1-40AF-99E7-45CD5E03C62B* .

55. Ministry of Communications and Information Technology, "Developing National Information Security Strategy for the Kingdom of Saudi Arabia --NISS, Draft 7," 26-29.

56. Ministry of Communications and Information Technology, "Anti-Cyber Crime Law," 2016, *http://www.mcit.gov.sa/En/AboutMcit/Regulations/Pages/CriminalLaws.aspx*.

57. Bureau of Experts at the Council of Ministers, "Anti-Cyber Crime Law," MCIT, 2009, *http://www.mcit.gov.sa/Ar/MediaCenter/Download/Anti_Cyber_Crime_Law_En.pdf*.

58. Freedom House, "Freedom on the Net 2016 – Saudi Arabia Country Profile," (2016).

59. Dino Wilkinson, "Saudi Arabia Updates Cybercrime Law to Include 'Naming and Shaming' Penalty," *Data Protection Report*, June 8, 2015, *http://www.dataprotectionreport.com/2015/06/saudi-arabia-updates-cybercrime-law-to-include-naming-and-shaming-penalty/*.

60. Freedom House, "Freedom on the Net 2016 – Saudi Arabia Country Profile," (2016).

61. Ibid.

62. "Communication Commission mandates companies to register fingerprints before issuing cards," [in Arabic] *Al-Riyadh Newspaper*, January 22, 2015, *http://www.alriyadh.com/1121516*.

63. Human Rights Watch, "Saudi Arabia: New Terrorism Regulations Assault Rights," March 20, 2014, *https://www.hrw.org/news/2014/03/20/saudi-arabia-new-terrorism-regulations-assault-rights*.

64. Ibid.

65. Eyad Reda and Turki Alsheikh, "Data protection in Saudi Arabia," *Thomson Reuters*, October 1, 2012, *https://uk.practicallaw.thomsonreuters.com/4-520-9455?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1*.

66. Melissa Hathaway, "Cybersecurity: The Intersection of Law, Policy and Technology," remarks given at the American Bar Association meeting, June 1, 2017.

67. Ministry of Communications and Information Technology, "Developing National Information Security Strategy for the Kingdom of Saudi Arabia – NISS, Draft 7," 14.

68. Fariborz Ghadar and Heather Spindler, "IT: Ubiquitous Force," *Industrial Management*, 2005, 14-20, *http://www.ghadar.byethost13.com/Images/IT-Ubiq_force.pdf?i=1*.

69. Rahayu Azlina Ahmad and Mohd Shamir Hashim, "The Organisation of Islamic Conference - Computer Emergency Response Team (OIC-CERT)," *Cyber security Summit (WCS), 2011 Second Worldwide*, 1-5, *http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5978783*.

70. Ministry of Communications and Information Technology, "Developing National Information Security Strategy for the Kingdom of Saudi Arabia – NISS, Draft 7," 2 and 61.

71. Ibid, 3.

72. Ibid, 61.

73. Ibid, 3.

74. Ibid, 13.

75. Eng. Abdullah Al-Swaha, "ICT Infrastructure Targeted in 1,000 Cyberattacks in 2016," *The Business Year.*

76. Ibid, 13.

77. KACST, "Communication and Information Technology Research Institute," *https://www.kacst.edu.sa/eng/RD/CITRI/Pages/AboutCITRI.aspx*.

78. Rabih Dabboussi, "DarkMatter to Underpin Importance of Digital Infrastructure Resilience at IDC CIO Summit 2016, KSA," *DarkMatter,* 2016, *https://darkmatter.ae/en/press_releases/48*.

79. Oxford Business Group, "Saudi Telecoms Companies Innovate in a Challenging Market," 2015, *http://www.oxfordbusinessgroup.com/overview/finding-their-calling-companies-are-innovating-challenging-market*.

80. Mohammed Rasooldeen, "SABIC launches innovation hub," *Arab News*. May 28, 2016, *http://www.arabnews.com/node/930916/saudi-arabia*.

81. Virginia Economic Development Partnership, *Cyber Security Export Market: Saudi Arabia*, George Mason University School of Public Policy, 2014, *http://exportvirginia.org/wp-content/uploads/2014/02/Saudi-Arabia.pdf*.

82. Raytheon Company, "Raytheon in Saudi Arabia," *http://www.raytheon.com/ourcompany/global/middle_east/raytheon_in_saudi_arabia/*.

83. Raytheon Company, "Raytheon and Saudi Arabia Military Industries announce strategic partnership," *PR Newswire*, May 20, 2017, *http://www.prnewswire.com/news-releases/raytheon-and-saudi-arabia-military-industries-announce-strategic-partnership-300461082.html*.

84. White House, "United States-Gulf Cooperation Council Second Summit Leaders Communique," Riyadh, Saudi Arabia, April21, 2016, *https://obamawhitehouse.archives.gov/the-press-office/2016/04/21/united-states-gulf-cooperation-council-second-summit-leaders-communique*.

85. U.S. State Department, "Fact Sheet: US Security Cooperation with Saudi Arabia," January 20, 2017, *https://www.state.gov/t/pm/rls/fs/2017/266861.htm*.

86. Bill Leigher, "Saudi Arabia Springs into Cyber Action," May 2015, *http://www.raytheoncyber.com/news/feature/saudi_cyber.html*.

87. Mark Sutton, "ICSC to Discuss Saudi Cybersecurity," November 6, 2016, *http://www.itp.net/610073-icsc-to-discuss-saudi-cyber%20security*.

88. Karen Elliott House, "Saudi Arabia in Transition," *Belfer Center for Science and International Affairs at the Harvard Kennedy School*, July 21017, *https://www.belfercenter.org/publication/saudi-arabia-transition*.

89. Ministry of Foreign Affairs, "Saudi Arabia and the Visit of President Trump," June 2017, *https://www.saudiembassy.net/sites/default/files/WhitePaper_TrumpVisit_June2017.pdf*.

90. Tan Sri Dato' Seri Panglima Mohd Azumi, "OIC-CERT: Past, present and future," *OIC-CERT*, December 14, 2016, *https://www.oic-cert.org/event2016/files/Attachment%204%20-%20Keynote%20Address.pdf*.

ABOUT THE AUTHORS

Melissa Hathaway is a leading expert in cyberspace policy and cyber security. She served in two US presidential administrations, spearheading the Cyberspace Policy Review for President Barack Obama and leading the Comprehensive National Cybersecurity Initiative (CNCI) for President George W. Bush. Today, she is a Senior Fellow and a member of the Board of Regents at Potomac Institute for Policy Studies. She is also a Senior Advisor at Harvard Kennedy School's Belfer Center for Science and International Affairs, a Distinguished Fellow at the Centre for International Governance Innovation in Canada, a non-resident Research Fellow at the Kosciuszko Institute in Poland, and she is President of Hathaway Global Strategies LLC, her own consultancy. Melissa developed a unique methodology for evaluating and measuring national levels of preparedness for certain cyber security risks, known as the Cyber Readiness Index (CRI). The CRI methodology is available in Arabic, Chinese, English, French, Russian, and Spanish, and is being applied to 125 countries. The CRI country profiles of France, Germany, India, Italy, Japan, the Netherlands, Saudi Arabia, the United Kingdom, and the United States can be found at the following link: *http://www.potomacinstitute.org/academic-centers/cyber-readiness-index*. Having served on the board of directors for two public companies and three non-profit organizations, and as a strategic advisor to a number of public and private companies, Melissa brings a unique combination of policy and technical expertise, as well as board room experience to help others better understand the intersection of government policy, developing technological and industry trends, and economic drivers that impact acquisition and business development strategy in this field. She publishes regularly on cyber security matters affecting companies and countries. Most of her articles can be found at the following website: *http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html.*

Francesca Spidalieri Francesca Spidalieri is the co-principal investigator on the Cyber Readiness Index Project at the Potomac Institute for Policy Studies. She also serves as the Senior Fellow for Cyber Leadership at the Pell Center, at Salve Regina University, as a Distinguished Fellow at the Ponemon Institute, and as 2017 Transatlantic Digital Debates Fellow at New America and at the Global Public Policy Institute. Her academic research and publications focus on cyber leadership development, cyber risk management, cyber education, and cyber security workforce development. In 2015, she published a report, entitled *State of the States on Cybersecurity*, that applies the Cyber Readiness Index 1.0 at the US state level. All her additional studies and academic articles can be found at the following link: *http://pellcenter.org/cyber-leadership/*.

Dr. Fahad Alsowailm is a senior researcher from Saudi Arabia focusing on foreign direct investments and national and international security-related issues. Fluent in both Arabic and English, he has traveled extensively and considers learning a lifelong activity. He received both his Bachelor's degree in Business Administration and his Master of Science degree from the American University in Washington, DC. He continued his studies at the University of Hull in the United Kingdom where he received his Doctorate in International Management. Dr. Alsowailm is also an alum of the John F. Kennedy School of Government and the London Business School's Executive Education programs.

For more information or to provide data to the CRI 2.0 methodology, please contact:

CyberReadinessIndex2.0@potomacinstitute.org

The CRI 2.0 methodology is available in Arabic, Chinese, English, French, Russian, and Spanish, and is currently being applied to 125 countries.

The CRI country profiles of France, Germany, India, Italy, Japan, the Netherlands, Saudi Arabia, the United Kingdom, and the United States can be found at the following link:

http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.

POTOMAC INSTITUTE FOR POLICY STUDIES
901 N. Stuart St. Suite 1200, Arlington, VA 22203
www.potomacinstitute.org