

BY CHRISTINA PÖPPER, MICHAEL MANIATAKOS,
AND ROBERTO DI PIETRO

Cyber Security Research in the Arab Region: A Blooming Ecosystem with Global Ambitions

IN A REGION where political tensions are recurrent, the *strive for security* is crucial. This applies equally to the cyberspace, where the need for cyber security is magnified by the level of digitization and technical penetration that the Arab region is experiencing. For instance, the Internet penetration rate^a is generally higher than 90% and, in some cases such as Kuwait, UAE, and Qatar, approaches 100%. As such, many Arab countries have recognized that the security of cyberspace is an integral part of their economic systems and a matter of national security. This awareness has been followed by policies and actions: In the International Telecommunication Union's (ITU) Global Cybersecurity Index,^b the states of Oman, KSA, Egypt, and Qatar rank among the top-20

a See <http://bit.ly/3bHrmY9>

b See <https://www.internetworldstats.com/stats.htm>

countries globally—with a considerable part of the Arab countries consistently ranking higher than many European countries. The strive for cyber security is a global as much as a local—and also Arab—endeavor, and the Arab region is gaining pace in cyber security research efforts and achievements. In this article, we will survey the main initiatives related to cyber security in the Arab region, report on the evolution of the cyber security posture, and point to possible Pan-Arab and international collaboration avenues in cyber security research.

Cyber security can be considered as specific to the Arab region as computing itself: Many of the threats, software and hardware developments, and industrial endeavors relating to cyber security are not exclusively tied to the region but are instead of a global character due to the nature of digitalization.

However, the political, economic, cultural, and financial contexts of Arab countries create a particular environment for facing attacks and addressing cyber security issues. The way the Arab world responds to cyber security challenges—in a broad but common understanding encompassing also trust and privacy—does not happen without tension or regional specificity: for instance, the protection of families and the respect for family life are an integral part of the Arab culture, while the strive for privacy protection is neither rooted nor strongly manifested in everyday digital life in Arab countries. Furthermore, while certain Arab countries are well known for their strong financial standing and politically stable systems—some being at the forefront of creating digital societies—others are suffering from war, instability, corruption, and poverty, which creates a heterogeneous and fragmented environment for threats and defenses on various scales.

As an example, the countries in the Gulf region share a strong dependency of their GDP on the oil and gas industry. For instance, the oil and gas sector



accounts for roughly 87% of Saudi budget revenues, 60% of Qatar's GDP, 40% of Kuwait's GDP, and 30% for UAE's GDP, to cite a few. Moreover, the production sites are typically concentrated in specific, narrow geographic regions, and represent a critical asset for the cited countries. For instance, on September 14, 2019, drones were used to attack the state-owned Saudi Aramco oil processing facilities at Abqaiq (Biqayq in Arabic) and Khurais in eastern Saudi Arabia, while in 2012 the Shamoon virus (aka W32.Dist-Track) was used against national oil companies including Saudi Arabia's Saudi Aramco^c and Qatar's RasGas.^d A group named "Cutting Sword of Justice" claimed responsibility for an attack on 35,000 Saudi Aramco workstations, causing the company to spend more than a week restoring

their services. Computer systems at RasGas were knocked offline by an unidentified computer virus, with some security experts attributing the damage to Shamoon. In 2017, software commonly referred to as Triton^e was the first malware to attack an industrial control system directly (not the IT infrastructure, like Shamoon did) by attacking a Saudi Arabian petrochemical plant. The cited attacks had worldwide consequences, sending up the price of oil, with further cascading effects and their increasing sophistication is alarming, pointing to state-level actors.

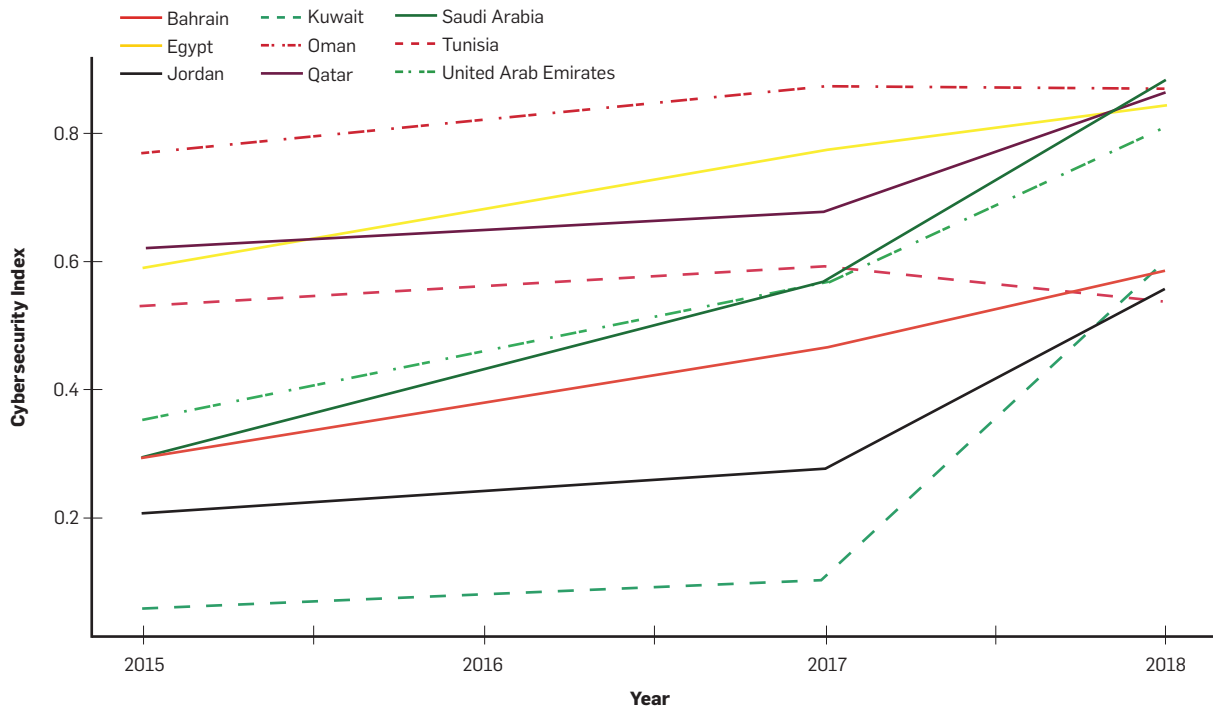
Consequently, awareness of the importance of cyber security raised within the national governments in the Arab region. One can observe committed endeavors toward the creation of secure digital environments within

Arab countries, manifested by the development of national cyber security strategies and the establishment of national cyber security agencies—at varying levels of maturity and scope (see accompanying table). National cyber security strategies exist or are in rollout for Egypt, Jordan, Lebanon, Kuwait, Qatar and the UAE, others have occurred as drafts or are in development (Saudi Arabia, Bahrain). For other Arab countries, the recognition of cyber security as a matter requiring a national strategy is gaining momentum. The endeavors have been well directed and managed, as shown by international benchmarks. For instance, ITU's cyber security index is overall rising in many Arab countries (see accompanying figure), indicating the national strategies, capabilities, and programs in the field of cyber security are on the rise (regarding national cyber security strategies and computer emergency response teams, but also

c See https://en.wikipedia.org/wiki/Saudi_Aramco
d See <https://en.wikipedia.org/wiki/RasGas>

e See [https://en.wikipedia.org/wiki/Triton_\(malware\)](https://en.wikipedia.org/wiki/Triton_(malware))

Evolution of ITU's Cyber Security Index for Arab countries with an index > 0.5 in 2018. For comparison, the curve for Europe displays the average index of all European countries with an index > 0.5 in 2018 (averaging 40 European countries).



cybercrime legislation, awareness, and capacity building).

Despite the efforts and results described here, Arab countries continue to be popular targets for cybercriminals, partially due to their financial power and oil resources, but also due to their location in a region rife with geopolitical tensions. Since the Arab region is situated at the crossroads of vastly different cultures, it has historically been a place of major geopolitical conflict, with impact on all Arab countries. With the transition to new ways of engaging into conflict,⁷ cyber security is essential in the modern cyber-defense landscape.

The Arab Research Landscape and Initiatives in Cyber Security

The importance of cyber security research has been recognized by national governments. One testimony of Arab research efforts in cyber security are the creation of academic research centers.

In the UAE, Abu Dhabi's long-term Vision 2030 outlines to promote a sustainable, diversified, high-value-added economy and the development of a resilient infrastructure capable of supporting anticipated economic

growth. Both will depend on high-tech infrastructures and interconnected computerized systems used everywhere in the country, for example, for smart grids and intelligent transportation. Relating to the secure realization of such a vision, NYU (New York University) Abu Dhabi's Center for Cyber Security, founded in 2012, pushes frontiers with respect to academic and industrial cyber-security research, with focus on hardware security, smart city security, wireless security, critical infrastructure security, and trust/privacy. Collaborative cyber security research is conducted together with the Center for Cyber-Physical Systems at Khalifa University.

On the northeastern coast of the Arabian Peninsula, the State of Qatar issued the Qatar National Vision 2030 that recognized cyber security as a strategic pillar. In this respect, the most recent effort is the creation of the Qatar National Agency for Cybersecurity that would provide a unified center for coping with cyber security threats. This last effort adds to the Qatar Computing Research Institute (QCRI) at Hamad bin Khalifa University (HBKU) that sports a Cyber

Security department, featuring research activities aimed at supporting governmental needs. Further, the very same HBKU has supported, within its College of Science and Engineering located just at the outskirts of Doha, the cited cyber security pillar creating the Cybersecurity Research and Innovation Lab that conducts research on a broad range of topics, with a focus on critical infrastructures protections (protection of avionics communications, maritime communication, drones and satellite security, and so forth). Further research efforts in cyber security are carried out at Qatar University and Carnegie Mellon University Qatar, mainly in the field of secure computing.

In Saudi Arabia, King Abdullah University of Science and Technology (KAUST) is pursuing a university-wide cyber-security initiative and is creating faculty positions at all levels in fields related to cyber security. The role played by KAUST in cyber security is magnified by the recent memorandum of understanding^f signed with

^f See <https://www.kaust.edu.sa/en/news/advancing-cybersecurity>

Saudi Arabia's National Cybersecurity Authority aimed at strengthening the cyber security capabilities of the Kingdom's workforce, focusing on developing educational programs in cyber security and providing consultations on curricula and training courses.

These exemplary and other initiatives bear fruit in connecting international cyber security researchers to the Arab region and in hosting existing and establishing new cyber security activities. In Feb 2020, the Global Cybersecurity Forum^g took place as an international two-day event in Riyadh, Saudi Arabia, concluding with the formulation of the Riyadh Declaration for Cybersecurity,^h being a commitment to cyber security objectives. November 2020 marked the 6th anniversary of the Cyber Security Awareness Week (CSAW) MENAⁱ region, organized by NYU Abu Dhabi. In 2019, HITB⁺ (Hack in the Box) CyberWeek^j took place for the first time, being the largest HITB cyber security event in the Middle East, followed by a virtual edition in 2020. CyberTalents, an Egypt- and UAE-based company has been organizing an Arab and Africa Cybersecurity CTF (Capture the Flag) competition yearly

g See <https://www.globalcybersecurityforum.com>
 h See <https://www.globalcybersecurityforum.com/declaration>
 i See <https://www.csaw.io/mena>
 j See <https://cyberweek.ae>

since 2017, currently covering ten Arab countries: Saudi Arabia, Oman, Sudan, Kuwait, Algeria, Morocco, Lebanon, Jordan, Tunisia, and Egypt. In 2019, Qatar's HBKU organized the first Qatar International Cybersecurity Contest, aiming at an interdisciplinary cooperation in cyber security—including social sciences, law, health sciences, Islamic studies and CS students—catalyzing more than 180 international participants. In terms of academic conferences, AsiaCCS 2017,^k ACM's Asia Conference on Computer and Communications Security, took place for the first time in the Arab region at NYU Abu Dhabi, hosting more than 200 international computer and cyber security researchers.

The liveliness of the cyber security ecosystem, and its global reach, is also testified by business success stories. For instance, DarkMatter, a UAE-based company that offers a complete portfolio of cyber security solutions underpins its work by industry-leading intelligence, research and development, resulting in the creation of the Technology Innovation Institute.^l In Qatar, the Qatar Science and Technology Park is home to a vibrant start-up ecosystem

k See <https://dl.acm.org/doi/proceedings/10.1145/3052973>
 l See <https://www.tii.ae>

Despite the efforts and results described here, Arab countries continue to be popular targets for cybercriminals, partially due to their financial power and oil resources, but also due to their location in a region rife with geopolitical tensions.

Overview of National Cyber Security Strategies (NCSS) and National Cyber Security Agencies/Bodies in selected Arab States. (See online appendix for notes and references <https://dl.acm.org/doi/10.1145/3447741>)

State	National Strategy			National Agency	
	NCSS available	Year of Creation	Current Coverage	Body available (since)	Name of Body
Bahrain	○ ^{1appx}	—	—	in development ^{1appx}	(MoI, iGA)
Egypt	● ^{7appx}	2017 (upd. in 2018)	2017–2021	✓ (2014)	ESCC ^{3appx}
Jordan	● ^{8appx}	2012	2018–2023	in development ^{8appx}	(MoICT)
Kuwait	● ^{9appx}	2017	2017–2020	in development ^{9appx}	NCSC
Lebanon	● ^{6appx}	2019	2019–2022	in development ^{6appx}	NCISA
Oman	◐ ^{4appx}	2017	—	✓ (2010)	OCERT ^{11appx}
Qatar	● ^{12appx}	2014	2014–2018	✓ (2020/21) ^{13appx}	NACS; Q-CERT(2005)
Saudi Arabia	◐ ^{2appx}	2013*	2013–2024	✓ (2017)	NCA ^{14appx}
Tunisia	◐ ^{15appx}	2018	2020–2025	✓ (2004)	ANSI ^{16appx}
UAE	● ^{10appx}	2019	2019–2022	in development ^{10appx}	(TRA); aeCERT (2008)

The liveliness of the cyber security ecosystem, and its global reach, is also testified by business success stories.

that enjoys generous funding and excellent logistics, aimed at incubating high tech start-ups, including the next stars of cyber security. In Egypt, the world's largest FinTech accelerator (Startupbootcamp) has put its root in Cairo, to foster innovation in financial inclusion and the general startup ecosystem, while local cyber security start-ups are growing up and, in a few promising cases, are acquired by international companies to boost their growth. A similar trend is experienced in the KSA. For instance, in 2019, Saudi Arabia's startup ecosystem saw an investment of \$67m, registering a 35% increase compared to a year before. The Kingdom also witnessed an increase in government initiatives, accelerator programs, and the total number of investors as well. All in all, the Arab region cyber security start-up ecosystem shows a clear positive trend, and it is poised to blooming.

Research Highlights and Awards

Among the many facets of cyber security, notable research environments and results relate to security for smart cities and critical infrastructures, maritime and aerial transportation security, hardware security, communication and Internet security, misinformation and fake news, as well as the use of AI for cyber security:

► *Hardware security:* NYUAD has created the world's first chip considered unhackable. Researchers of NYUAD's Design for Excellence (Dfx) lab developed a 'logic-locked' security chip to protect devices from the surge in cyber-attacks. Secured by a secret key, it permits only authorized users to utilize the device and it is also resistant to reverse engineering. The group's research was presented at the ACM Conference on Computer and Communications Security,¹⁷ one of the leading cyber security conferences in the world.

► *Smart city and critical infrastructure security:* NYUAD's Center for Cyber Security hosts a smart city testbed as an Internet of Things (IoT) platform with a collection of interoperable processes, simulation models, hardware devices, and appropriate network protocols. With application to smart grid, intelligent transportation, chemical plants, smart houses/buildings, and desalination plants, it is being used

to produce a series of offensive and defensive results in industrial control system security: It was used to identify power grid vulnerabilities^m (CVE-2017-7905, presented at BlackHat USA 2017), investigate GPS spoofing attacks possibly leading to time synchronization problems, demonstrate attacks on firmware modification of power grid devices and detect malicious modifications in the firmware of embedded systems.⁸ HBKU's College of Science and Engineering is home to the Cybersecurity Research and Innovation Lab (CRI-Lab)ⁿ that also performs research on the protection of critical infrastructures. The lab has strategic plans, advanced testbeds, and top-notch researchers to address IoT security¹³ and the application of AI techniques to relevant cyber security research problems.¹²

► *Aerial and maritime security:* HBKU's Cybersecurity Research and Innovation Lab also addresses maritime cyber security,³ avionics security,¹¹ and satellite security.⁹ Researchers from NYUAD's Cyber Security & Privacy Lab have developed DeepSIM, a technique to detect GPS spoofing attacks on UAV's using camera input and satellite imagery matching¹⁶ and MAVPro, an approach for ADS-B message verification for air traffic security that increases the geographic coverage of multilateration-based verification.⁵

► *Communication security and applied cryptography:* In an international team, scientists from Saudi-Arabia's KAUST published a paper in Nature Communications⁶ to demonstrate perfect secrecy cryptography in classical optical channels^o using chaos theory and the second law of thermodynamics, a possible response to the emergence of quantum computers and the risk this carries for classical cryptographic approaches. Their approach relies on correlated mixing of chaotic waves in an irreversible time-varying silicon encryption chip. In other international collaborations with first-tier publication results, NYUAD researchers analyzed the Dragonfly handshake of WPA3,¹⁵ the recent Wi-Fi security

m See <https://www.reuters.com/article/us-cyber-generalelectric-power-idUSKBN17S23Y>

n See <https://cri-lab.net>

o See <http://bit.ly/39zr4Qt>

standard that is replacing WPA2, and introduced a new paradigm for side-channel attacks over remote connections by exploiting concurrency to leak secrets.¹⁴ Qatar University and Carnegie Mellon University in Qatar are also addressing special topics in cyber security, such as the challenging endeavor of producing a viable sound prototype of a garbled computer—an appealing alternative to homomorphic encryption.¹⁰ HBKU-CSE's research in this domain addresses privacy² and cloud computing.⁴

► *Internet security*: With its Security Department, HBKU's research institute QCRI sports a number of initiatives in the cyber security field. It actively investigates relevant problems with worldwide impact, such as MADA:^p A system for identifying malicious domains using a real-life 'guilt by association' principle. It detects malicious domains by analyzing the movements and previous associations of a domain address—it can analyze 50 million domains in six minutes.

► *Misinformation and fake news*: Another branch of QCRI leads the Tanbih mega-project,^q developed in collaboration with MIT. The project aims to build a news aggregator that limits the effect of fake news, propaganda and media bias—a key tool for the Arab region given the high Internet penetration as described at the beginning of this article, combined with the fact that the vast majority among the young Arab generations consume online news.

► *AI for cyber security*: QCRI has also helped define the AI strategy for Qatar,^r a cornerstone element to address current and future challenges of cyber security.

Cyber security research is also conducted in Lebanon, where the research group led by Ali Chehab at the American University of Beirut is addressing topics from SDN security, to physical-layer security, and network coding. At the other end of the spectrum is Egypt, where cyber security is a key topic for the industrial sector, with collaborations in place with top indus-


trial players like Siemens and Valeo.

Finally, research highlights from the Arab region include recent awards relating to cyber security. In 2020, a Google Ph.D. Fellowship in Privacy and Security went to Yunusa Simpa Abdulsalm from Mohammed VI Polytechnic University in Morocco, who is working on securing the electronic health system. With this selection, the Google Ph.D. Fellowship was awarded for the first time ever to the Arab Region on a cyber security topic. In 2020, Naif Saleh Almakhdhub, Assistant Professor of Engineering at KAUST in Saudi Arabia, received the CSAW MENA award for his NDSS 2020 paper on a compiler-based mitigation to prevent control-flow hijacking attacks for securing embedded systems.¹ In 2019, Amer Al Jaberi from the UAE received the MIT Technology Review MENA Region Innovator Under 35 distinction for a document and passport reader being used by all immigration portals in the UAE, verifying the veracity of the documents while safeguarding the various ports of entry from fraud. The young academics and engineers are raring to go.

Our Vision for the Future of Cyber Security in the Arab Region

The cyber security landscape for the Arab region presents unique challenges and opportunities. The importance of cyber security is well represented in the national policies, funding is provided to adequately address the challenges of choice, and a vibrant research ecosystem in cyber security is gaining more and more momentum. However, the efforts for creating secure digital environments and establishing research excellence in cyber security in Arab countries are still often reactive and fragmented. The high level of dependency on few key critical infrastructures (namely the oil and gas sector) and the level of threats that the countries in the region are facing, call for further collaborative actions to devise solutions idiosyncratic to this unique context.

In particular, the need for further coordination, sharing of best practices and experiences, boosting research excellence, and the creation of specific transnational research

projects aiming at solving specific issues shared by countries in the region would be highly beneficial for the whole region and will reinforce the Arab region experience in cyber security as a model for the rest of the world. This will take time but invoke irreversible benefits for the region. Finally, to unleash the Arab region potential, we emphasize the importance of an excellent cyber security training and education infrastructure, including academic cyber security programs and specializations. 

References

- Almakhdhub, N.S. et al. RAI: Securing embedded systems with return address integrity. NDSS 2020.
- Bentafat, E., Rathore, M. and Bakiras, S. A practical system for privacy-preserving video surveillance. ACSAC 2020.
- Caprolu, M. et al. Vessels cybersecurity: Issues, challenges, and the road ahead. *IEEE Commun.* 58, 6 (2020), 90–96.
- Chkribene, A. and Erbad, R. Hamila: A combined decision for secure cloud computing based on machine learning and past information. *IEEE WCNC* 2019.
- Darabseh, A., Alkhzaimi, H., and Pöpper, C. MAVPro: ADS-B message verification for aviation security with minimal numbers of on-ground sensors. *ACM WiSec* 2020, 53–64.
- Di Falco, A. et al. Perfect secrecy cryptography via mixing of chaotic waves in irreversible time-varying silicon chips. *Nature Communications* 10, 5827 (2019). <https://doi.org/10.1038/s41467-019-13740-y>
- Di Pietro, R. et al. *New Dimensions of Information Warfare*. Springer International Publishing, 1st Ed. (2021); <https://doi.org/10.1007/978-3-030-60618-3>
- Keliris, A. and Maniatakos, M. ICSREF: A Framework for Automated Reverse Engineering of Industrial Control Systems Binaries. NDSS 2019.
- Oligeri, G., Sciancalepore, S., and Di Pietro, R. GNSS spoofing detection via opportunistic IRIDIUM signals. *ACM WiSec* 2020, 42–52.
- Rachid, M.H., Riley, R. and Malluhi, Q.M. Enclave-based oblivious RAM using Intel's SGX. *Comput. Secur.* 91, 101711 (2020).
- Sciancalepore, S. and Di Pietro, R. SOS: Standard-compliant and packet loss tolerant security framework for ADS-B communications. *IEEE Transactions on Dependable and Secure Computing* (2019); <https://doi.org/10.1109/TDSC.2019.2934446>
- Sciancalepore, S. PiNCh: An effective, efficient, and robust solution to drone detection via network traffic analysis. *Comput. Networks* 168 (2020).
- Tedeschi, P. et al. LiKe: Lightweight Certificateless Key Agreement for Secure IoT Communications. *IEEE Internet Things J.* 7, 1 (2020), 621–638.
- van Goethem, T. et al. Timeless timing attacks: Exploiting concurrency to leak secrets over remote connections. In *Proceedings of the USENIX Security Symposium 2020*: (2020), 1985–2002.
- Vanhoef, M. and Ronen, E. Dragonblood: Analyzing the Dragonfly handshake of WPA3 and EAP-pwd. In *Proceedings of the IEEE Symposium on Security and Privacy 2020*, 517–533.
- Xue, N. et al. DeepSIM: GPS spoofing detection on UAVs using satellite imagery matching. ACSAC 2020.
- Yasin, M. et al. Provably-secure logic locking: From theory to practice. *ACM CCS* 2017, 1601–1618.

Christina Pöpper, NYU Abu Dhabi, UAE.

Michail Maniatakos, NYU Abu Dhabi, UAE.

Roberto Di Pietro, HBKU-CSE, Doha-Qatar.

The information and views in this article are those of the authors and do not necessarily reflect the official opinion of their institutions.

© 2021 ACM 0001-0782/21/4

p See <https://www.hbku.edu.qa/en/research-groups/cyber-security>

q See <http://tanbih.qcri.org>

r See https://qcai.qcri.org/wp-content/uploads/2019/10/QCAI_MOTC_AI_Strategy_English_FINAL.pdf