Cybersecurity in Saudi Arabia

Author: dr Aleksander Olech
Analytical support: Karolina Siekierka

11.08.2021

Main points:

- Saudi Arabia has the largest information and communication technology (ICT) market in the Middle East and the country is constantly developing it.
- In 2020, Saudi Arabia recorded over 22,5 million cyber attacks, each of which cost 6,5 million dollars to the state.
- In March 2021, the Ministry of Education of Saudi Arabia and the National Cybersecurity Authority signed an agreement on launching joint training and research programs in the field on cybersecurity.
- Since the first cyber attack on Saudi Aramco, Saudi Arabia has introduced a series of measures aimed at reducing the occurrence of cyber attacks.

Challenges and competition in a context of billions-worth of investments

Saudi Arabia is undergoing domestic developments focused on expanding its cyberspace capabilities. This process has been accelerated by the COVID-19 pandemic and by the drastic fall of oil prices. **Already in 2016, in the framework of the Saudi Vision 2030 strategy, it had been emphasized that the Kingdom of Saudi Arabia (KSA) intends to reduce its dependence on oil, diversify its economy, and develop public service sectors, such as the health, education, infrastructure, recreation and tourism sector.** The core of this initiative consists in a focus on technology, digital transformation, and the development of digital infrastructure. Essentially, the strategy itself does not deal either with cyberspace or cyberterrorism issues[1], but it indicates the path for changes.

At the beginning of the coronavirus pandemic in the first quarter of 2020, the Middle Eastern countries experienced an increase in malware attacks by 22% and in spam attacks by 36%. It was a particularly difficult period for the companies in Saudi Arabia, which were undergoing the process of converting to remote work[2]. ICT infrastructure in both the public and private sector are constantly threatened by cyber incidents due to Saudi Arabia’s strategic position in the region. These cyber attacks have a huge impact on economy at the financial, operational,

[1] Kingdom of Saudi Arabia, *Saudi Vision 2030*, Government of Saudi Arabia, Riyadh 2016

[2] A. Buller, *Saudi Arabia sees cyber security boom as coronavirus bites*, Computer Weekly, 17.09.2020, accessed: 16.07.2021

and tactical level, which can potentially weaken the citizens' trust in government services and in authority itself[3]. Consequently, this may affect the country's political stability and lead to further attacks by cybercriminals from neighbouring states.

Private and public institutions in Saudi Arabia also faced the challenge of work organisation in times of COVID-19 pandemic. The emerging risk of losing sensitive data sent by employees working from home resulted in the reorganisation of the IT domain in the whole country. The compulsory blockade to stop the spread of the virus caused all forms of communication to be transferred to the internet. They enforced the rule of holding meetings on Zoom, making online purchases and conducting virtual education. Thus far, in Saudi Arabia the custom of working at the office and organising meetings in person had been predominant. The dynamic change in the operating policy of virtually all companies in the country resulted in calls for the rapid implementation of strategies enabling employees to maintain a good level of productivity. This involved moving data to data clouds and granting access to remote IT resources of enterprises. As a result, it was necessary to increase the security level in cyberspace by investing in new technologies and implementing security measures resistant to external attacks. Another important element was training employees[4], who have access to the company data, so that they also constantly analyse emerging threats and follow safety rules[5].

More than one half of the Saudi directors of information affairs consider security management as the greatest technological challenge, and investing in cybersecurity as a key business goal. Moreover, the necessity to maintain cybersecurity has become one of the main indicators of companies performance and digital transformation in the whole country, which means that expenditure on technologies and protection against data leakage will get higher from year to year[6].

[3] A. Quadri, M. K. Khan, *Cybersecurity challenges of the Kingdom of Saudi Arabia: Past, Present and Future*, Global Foundation for Cyber Studies and Research, January 2019, p. 7

[4] A. Alzubaidi, *Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia*, Heliyon, Vol. 7, 1st edition, 2021

[5] A. Buller, *Saudi Arabia sees cyber security boom as coronavirus bites*, Computer Weekly, 17.09.2020, accessed: 16.07.2021

[6] B. Wright, K. Allan, *Saudi CIOs consider security their toughest tech challenge, CIO, 25.08.2020*, https://www.cio.com/article/3445225/saudi-arabias-cybersecurity-concerns-increase-as-threats-evolve.html, accessed: 18.07.2021

Cyberterrorism threats

In 2015, Saudi Arabia faced 160,000 attacks a day[7]. The country is attacked much more often than other countries in the region due to its international position and its resources. Such intensification of threats causes difficulties in the functioning of both the public and private sector. Cyber attacks of different scale and intensity can considerably damage the economy and negatively affect the social and political stability of the country. What is more, cybercrime is also one of the main causes of huge money financial prestige loss.

Cyberspace protection currently represents one of the most important challenges in ensuring the security and stability of states. Since 2006, there has been a significant increase in attacks on their critical infrastructure, which plays an important role in the functioning of the state and civil society. They can take different forms and are aimed at, for example, gaining insight, stealing or destroying highly guarded information, and disrupting the activity of files or computer systems by introducing malicious software. **In 2012 alone, the Kingdom lost 693 million dollars, while this amount gets higher year by year[8]. In 2020, Saudi Arabia recorded over 22,5 million such attacks[9], each one costing the state 6,5 million dollars[10], while in the first quarter of 2021 over 7 million cyber attacks were registered[11].** The American Centre for Strategic and International Studies reports that of all the attacks carried out between May 2006 and June 2020, 15 posed a significant threat to national security. In the 2020 Cybersecurity Exposure Index rankings and in the 2020 Cyber Risk Index, Saudi Arabia was ranked respectively 31st[12] and 25th-26th[13] on a global scale.

[7] Arabian Business, *160,000 cyberattacks a day in Saudi Arabia*, https://www.arabianbusiness.com/160-000-cyberattacks-day-in-saudi-arabia-630120.html, accessed: 20.07.2021

[8] A. Quadri, M. K. Khan, *Cybersecurity challenges of the Kingdom of Saudi Arabia: Past, Present and Future*, Global Foundation for Cyber Studies and Research, January 2019, p. 7

[9] T. Nasarallah, *Saudi Arabia: over 7 million cyberattacks foiled in 3 months*, Gulf News, https://gulfnews.com/photos/lifestyle/photos-fashion-abayas-by-safia-hussain-showcased-in-riyadh-1.1611420228808?slide=6, accessed: 16.07.2021

[10] C. Kelly, *IBM: Cyber breaches cost enterprises in the UAE and KSA over $6.5m per attack in 2020*, ITP, https://www.itp.net/news/93473-ibm-cyber-breaches-cost-enterprises-in-the-uae-and-ksa-over-65m-per-attack-in-2020, accessed: 16.07.2021

[11] T. Nasarallah, op. cit.

[12] J. Frisby, *Cybersecurity Index (CEI) 2020*, PasswordManagers.co, https://passwordmanagers.co/cybersecurity-exposure-index/, accessed: 16.07.2021

[13] NordVPN, *Cyber Risk Index*, 2020, https://s1.nordcdn.com/nord/misc/0.13.0/vpn/brand/NordVPN-cyber-risk-index-2020.pdf, accessed: 16.07.2021

Attacks on the Saudi Arabian cyberspace

One of the most threatening attacks on national cyberspace took place in August 2012, when the virus Shamoon was introduced into the internal communication network of the state-owned oil company Saudi Aramco. Its aim was to stop the oil and gas production and weaken the largest company in the Middle East energy market. As a result of this incident, more than 30,000 computers were damaged and all data on their disks were deleted and replaced with a picture of a burning American flag. In order to stop the spread of the virus, Saudi Aramco was forced to stop working and blocked both the email and internet access of all employees. This stopped the activity of the company for two weeks and caused huge financial losses. During the five-months shutdown, the cybersecurity team carried out activities aimed at implementing new solutions to maintain cybersecurity. The attack posed a threat not only to Saudi Arabia itself, but also to Western countries, in particular those dependent on AS oil supply. Despite the lack of evidence, the US intelligence accused Saudi Arabia's greatest rival in the region, the Islamic Republic of Iran, of having attacked.

Another attack on Saudi Aramco, inflicted this time with the updated Shamoon 2 virus, took place in August 2017. The company stopped working for 48 hours. The significantly shorter business activity pause was due to the company's decision, made after 2012, to constantly store backups. **According to the New York Times, the purpose of the cyberattack was to trigger an explosion and sabotage the entire system[14]. The identity of the responsible for the attack has not been confirmed, but Iran has also been accused in this case.**

In December 2019, Saudi government bodies detected a cyberattack planned on Saudi Arabia's critical structure. The Dustman malware, permanently deleting data stored on disks, was used during the attack. It was uncertain which state bodies were to be targeted, as the traces left by the hackers suggested that the attack was hastily organised. More importantly, it took place in conjunction with the escalation of tensions on the Iranian-American front. According to CyberScoop, whose article bases its assumption on the political situation, the similar manners

[14] N. Perlroth, C. Krauss, *A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try*., The New York Times, https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html, accessed: 16.07.2021

in which the attacks were carried out and the traces left, the responsible party was the Iranian hackers[15].

Saudi Arabian state authorities and companies are not the only targets of attacks that result in deletion or blocking of information. In May 2020, the Kingdom of Saudi Arabia was victim of an unsuccessful espionage campaign led by the Iranian entity Chafer APT. It was directed at the Saudi critical infrastructure, and in particular at the telecommunication and tourism sectors that store a significant amount of personal data, as well as at the government administration. The purpose was, among others, to gather data on credentials for espionage purposes[16].

What is more, contemporary trends in Saudi Arabia indicate that cyber terrorists are using social media as an alternative to disrupt communication between citizens and hinder the economic activity by penetrating users' communication channels. Moreover, they use the network to recruit adepts, raise funds and conduct disinformation campaigns on Saudi Arabia. **As many as 30,2 million citizens (91% of the population) have access to the internet and 25 million have an account on a social network. Currently, the media most often cracked by terrorists are WhatsApp, YouTube, Facebook, Instagram, and Twitter[17].**

Cybersecurity strategy

In the light of the contemporary challenges for cybersecurity, **the Royal Decree of October 31st, 2017 established the National Cybersecurity Authority (NCA), whose main task is to increase the state's cybersecurity by preparing internal analysis and legal solutions. The office consists of the head of the Presidency of State Security, the head of the General Intelligence Presidency (GIA)[18]**, the Deputy Minister of Internal Affairs, and the Deputy

[15] S. Lyngaas, *Saudi cyber authority uncover new data-wiping malware, and experts suspect Iran is behind it*, CyberScoop, https://www.cyberscoop.com/saudi-arabia-iran-cyberattack-soleimani/, accessed: 17.07.2021

[16] B. Rusu, *Iranian Chafer APT Targeted Air Transportation and Government in Kuwait and Saudi Arabia*, Bitdefender, https://www.bitdefender.com/files/News/CaseStudies/study/332/Bitdefender-Whitepaper-Chafer-creat4491-en-EN-interactive.pdf, accessed: 17.07.2021

[17] Skillzme, *Saudi Arabia Social Media Statistics 2018*, https://skillzme.com/ksa-social-media-statistics-2018, accessed: 17.07.2021

[18] The General Intelligence Presidency is the Saudi security body, established in 2017, which supervises simultaneously the activities of national anti-terrorist and intelligence services.

Minister of Defence[19]. The NCA performs both regulatory and operational functions related to cybersecurity and it also closely cooperates with public and private entities to improve the country's security, protect its interests, critical infrastructure, and build a cyberspace environment for the implementation of the 2030 strategy[20].

The NCA developed a strategic cybersecurity vision that reflects the Saudi Arabia's goals, which are the creation of conditions in cyberspace to maintain security, trust in the authorities, and technological growth. The priority goals for 2030 encompass six aspects[21]:

- Harmonisation of cybersecurity throughout the country - ensuring high-level coordination and guideline adjustment in all the subordinated entities; it is important to adopt a comprehensive state approach to cybersecurity through integration, clear definition of roles and responsibilities of the actors at a national level to develop and implement regulations and policies, and compliance with national standards.

- Risk management – identifying targets in cyberspace and detecting damages; subsequently, verifying the most appropriate methods of risk elimination in order to reduce the negative effects.

- Optimal functioning in the cyberspace environment – introducing comprehensive controls, national norms and a compliance monitoring system that will ensure the protection of the cybersecurity environment, including raising the level of social awareness of cyber threats.

- Dynamic defence – strengthening and constantly developing national capabilities in the field of defence against cyber threats; detecting, preventing, responding and reorganising after attacks.

- International partnership – cybersecurity requires stable local partnerships, strengthened by advanced information exchange mechanisms, which allows for the

[19] Saudi Gazette, King orders setting up of National Cyber Security Authority, https://saudigazette.com.sa/article/520782/SAUDI-ARABIA/King-orders-setting-up-of-National-Cyber-Security-Authority, accessed: 17.07.2021

[20] National Cybersecurity Authority, Essential Cybersecurity Controls, 2018, pp. 6-10

[21] National Cybersecurity Authority, National Cybersecurity Strategy (Overview), Kingdom of Saudi Arabia, December 2020, pp. 14-29

improvement of systems and the exchange of best practices; in order to achieve the required level of security, efforts should be made to strengthen foreign partnership.

- Cyberspace development – efforts should be made to increase national capabilities in the field of cybersecurity, and one of the main paths to be undertaken are investments in education and training, as well as in industry and research.

Moreover, in view of the size of the Saudi economy, the Kingdom focused on creating government structures that would make it possible to use the state's potential and counteract emerging threats. Thus, in 2019 Saudi Arabia created another three bodies that are related to the NCA. **The Saudi Data and Artificial Intelligence Authority (SDAIA) is responsible for the elaboration of data storage strategies and development of artificial intelligence, as well as for the National Centre for Artificial Intelligence and the Saudi Commission for Data and Artificial Intelligence, which are subordinated to it.** Such actions are a clear manifestation of the Kingdom's determination to expand its digital capabilities and build a future based on artificial intelligence and innovation. According to Saudi authorities, artificial intelligence will increase productivity, improve decision-making processes in all sectors, provide more innovative services to citizens and allow businesses to grow[22]. It is also worth noting that Saudi Arabia is constantly updating the 2007 Cyber Crime Law.

A new cyberspace deal

In March 2021, the Ministry of Education of Saudi Arabia and the National Cybersecurity Authority signed an agreement to launch joint training and research programs in the field of cybersecurity. This is of great importance in terms of investing in cybersecurity initiatives and it is part of the realisation of the 2030 Strategy. The Ministry of Education and the NCA are already implementing several joint projects on scholarships for cyberspace research and the development of higher education in the domain of cybersecurity[23].

Since the first cyber attack on Saudi Aramco, Saudi Arabia has introduced a series of measures to reduce the occurrence of cyber attacks. One of these is the government's decision to double

[22] A. Gernonimo, National Centre for AI to drive Saudi Arabia's digital future: minister, TahawulTech, 01.09.2019

[23] Arab News, Deal signed to boost cybersecurity education in Saudi Arabia, https://www.arabnews.com/node/1830711/saudi-arabia, Homepage 24.03.2021, accessed: 17.07.2021

the cybersecurity budget. **Back in 2012, these expenditures increased from 7,8 to 15,4 billion dollars[24], while in 2020 they reached the amount of 27,2 billion[25]. In 2014, they established the National Centre for Cybersecurity Technology, a research and development institution dealing with network, software, and information security issues.** The analysis elaborated by the Centre is to prepare the country for the implementation of the "Vision 2030" project.

The state cooperates in the field of cybersecurity both with international organisations (including the United Nations and the League of Arab States) and on the basis of bilateral agreements (for example with the United States, Great Britain, and the United Arab Emirates), but in the light of the tensions in the relations with Iran and the related increase in the number of cyber-attacks, it is most active in the Gulf Cooperation Council, where it initiates discussions on extending cooperation in the field of cybersecurity. **The number of actors Saudi Arabia cooperates with is limited since the state considers the issue of cybersecurity as a small element of its foreign policy[26], instead being rather focused on internal security as a key aspect.**

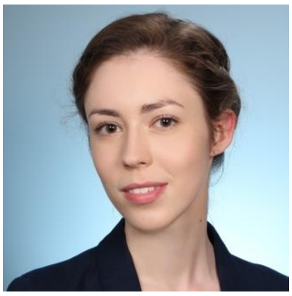
[24] S. Alshathry, Cyber Attack on Saudi Aramco, "International Journal of Management and Information Technology", 2017, Vol. 11, No. 5, p. 3039

[25] USSABC Economic Brief: Saudi Arabia's Emergence in Cyber Technology, U.S.-Saudi Arabian Business Council, http://ussaudi.org/wp-content/uploads/2020/01/Economic-Brief-Saudi-Cybersecurity-Leadership.pdf, accessed: 17.07.2021

[26] Saudi Arabia's Foreign Policy Priorities, Chatham House, https://chathamhouse.soutron.net/Portal/DownloadImageFile.ashx?objectId=3483, accessed: 17.07.2021

ABOUT THE AUTHORS

Dr Aleksander Olech. Director of the European Security Programme at the Institute of New Europe. PhD in security studies. Specialist in the field of security and international relations. He gained research experience at the Université Jean Moulin III in Lyon, the Institute of International Relations in Prague, and the Institute of Peace Support and Conflict Management in Vienna. Scholarship holder of the OSCE & UNODA Peace and Security Program and the Casimir Pulaski Foundation. His main research interests are terrorism, international cooperation for security in Eastern Europe and the role of NATO and the EU with regards to hybrid threats.



Karolina Siekierka. MA student of International Relations, specialization in Security and Strategic Studies, Faculty of Political Science and International Studies, University of Warsaw. During her studies she participated in student exchanges with Université Panthéon-Sorbonne (Paris 1) and Institut d'Etudes Politique de Paris (Sciences Po Paris). Her research interests include international law, international political relations and human rights. She is involved in student organizations at the University of Warsaw and Sciences Po.

NIW
Narodowy Instytut Wolności
Centrum Rozwoju Społeczeństwa Obywatelskiego

Sfinansowano przez Narodowy Instytut Wolności - Centrum Rozwoju Społeczeństwa Obywatelskiego ze środków Programu Rozwoju Organizacji Obywatelskich na lata 2018 – 2030

Program Rozwoju Organizacji Obywatelskich na lata 2018–2030
PROO

IF YOU VALUE THE INSTITUTE OF NEW EUROPE’S WORK, BECOME ONE OF ITS DONORS!

Funds received will allow us to finance further publications.

You can contribute by making donations to INE’s bank account:

95 2530 0008 2090 1053 7214 0001

with the following payment title: „darowizna na cele statutowe”\