Jansta Associates
LIMITED

PHYSICAL SECURITY

MARKET & TECHNOLOGY OVERVIEW

Kingdom of Saudi Arabia

JA/Research/KSA/001

R01

Date: 29/06/2021

+44 (0) 789 685 92 44
www.janstaassociateslimited.com
twitter.com/peter jansta
UK, Europe, Middle East & Asia

Table of Contents

1. INTRODUCTION

The turmoil and ongoing conflicts in Iraq, Syria and Yemen are forcing Saudi Arabia's government to spend "whatever it takes" to secure its stability and defeat any internal or external threats. Saudi Arabia's defence and security expenditures reached 57.5 billion in 2020. [1]

Opportunities have emerged in the market for personal and perimeter security products. Other growth areas are contracts through technology transfer, spare parts manufacturing, security training programs, intelligence, surveillance, reconnaissance (ISR), and unmanned aerial vehicles (UAV).

A need for expertise in cybersecurity also increases with the growing sophistication of threats. Forecasts indicate that the market will reach a value of $5.1 billion by 2022. [2]

Rising government initiatives in line with Vision 2030 and increasing IT spending drive rapid growth in the physical security market segment (see fig.1). The security industry is facing a huge disruption. Cloud computing, AI and IOT are blurring the line between logical and physical environments.

Fig.1: *HLS & PS Market*

Digital transformation of physical security is still in its infancy in comparison to other industries. As tools become more sophisticated and readily available, security organisations must adopt new practices and capabilities. Failure to transform will increase the likelihood of becoming a target. Top investments over the next 3-5 years are big data and analytics, cloud computing and storage, and the Internet of Things (IoT). The future of physical security with digital transformation will be drastically different from physical security today.

This report intends to provide a snapshot of Saudi homeland security, focusing on physical security, highlighting submarkets that will provide attractive business opportunities and the market size and trends during 2021-2023.

2. TECHNOLOGY

The seismic shifts set out by ambitious Vision 2030 are unprecedented. For example, NEOM city is a large project that dwarfs most mega projects in the region. The objective is to create an environment that will set a precedent for future humanity; how is that for a start.

When closely examined, the focus is on urban planning, technologies, and sustainability. As with any project in the region, security plays a pivotal part, and technology is as important as overall processes. In this section, we will examine some existing as well as fast-approaching changes in the region.

2.1 Border Security

Saudi Arabia has disaffected minorities susceptible to outside influence and can help enemies breach the country's borders. For example, the Shia communities of the Eastern Province and in the southern Asir Province. The terrain along the land borders is desert with varying types of sand and terrain features. However, the border areas are generally open, with vast stretches of desert that are inhospitable because of climate and lack of infrastructure.

To secure their perimeters, the Saudis have built a fence and an earthen berm along both their northern border with Iraq and their southern border with Yemen. International intelligence-sharing capabilities are critical to border security efforts. Outreach to allies is an effective way of learning about what is happening beyond the immediacy of security at the border and gaining early warning of a threat. Comprehensive situational awareness of security along the borders will depend on reaching out to allies and sharing information with other nations beyond a country's immediate neighbours.

New technologies and equipment are helpful, provided they are maintained and used correctly, and operators and forces are adequately trained. The government requires integrated information technology and communication system with coordinated procedures and processes. Without these, security forces will be unable to respond effectively in a crisis. Dust and rugged ground in the desert can wreak havoc on equipment, requiring the additional expense of replacing hardware frequently than under normal working conditions. Once systems and physical security barriers and procedures are operational, practice and training are necessary to maintain adequate proficiency levels. This is particularly true where new technologies, such as drones, biometrics, and pattern- recognition software, are being used. Without practice and training, there will be a loss of agility in response time and an overall loss in system resiliency.

2.2 AI Surveillance Technology

AI surveillance technology is spreading at a faster rate to a wider range of countries than experts have commonly understood. At least seventy-five out of 176 countries globally are actively using AI technologies for surveillance purposes. For example, Huawei is helping the government build safe cities[3]. Google is establishing cloud servers, and BAE provides surveillance systems. NEC is vending facial recognition cameras. Amazon and Alibaba both have cloud computing centres to support a major smart city project.

Saudi Arabia's Makkah Region Development Authority (MRDA) created a crowd-control system to increase the safety and security of Hajj pilgrims. Data is collected via a wristband embedding identity information, special healthcare requirements and a GPS. In addition, surveillance cameras are installed to collect and analyse real-time video along the Al Mashaaer Al Mugaddassah Metro Southern Line (MMMSL) and the holy sites.

2.3 Biometric Identification

The biometrics market is projected to cross $52 million by 2024. The biometrics enabled visas and passports are mandatory for all visitors entering the country. Saudi government recognised the pressing need to allow swift and irrefutable proof of identity. Digital IDs have been issued to 17 million people in Saudi Arabia through the Interior platform to help them access government services.

The government digital identity program provides access to 147 different platforms and service portals, granting online access to more than 200 services. Biometrics are becoming an increasingly important component of security-related applications, including logical and physical access control, airport, sea security, border control, forensic investigation, IT security, identity fraud protection and terrorist prevention or detection.

2.4 CCTV

Saudi Arabia is emerging as one of the fastest-growing CCTV markets in the Middle East region. The demand for CCTV has increased on account of rising government initiatives, increasing IT spending, and the hospitality sector's growth. The market for CCTV is benefiting from the increasing adoption of IP based systems in various industries and enterprises, the rising need for security/surveillance systems, and growing infrastructure development projects.

2.5 Access Control Systems

Access Control Systems market in Saudi mainly consists of access cards, biometrics-based systems and controllers. The country's ACS market is showing solid signs of growth, which can largely be attributed to increasing government expenditure on security infrastructure to curb the rising crime rate, fraud, and terrorist attacks. The major players in the market are Bosch Security Systems, Johnson Controls, Siemens, Honeywell, Genetec, NEC Corporation, Nedap, IrisGuard, 3M Cogentand Cisco Systems.

A prominent trend is the rising use of physical access control systems and IT security on a single platform. In addition, centralised credential management across the security infrastructure helps enhance a company's operational efficiency. Organisations are increasingly migrating from analogue to IP-enabled physical access control systems to improve operational efficiency, security, and availability.

2.6 Cloud Computing

While Saudi Arabia is still in the early stages of adopting cloud computing, an increasing number of IT decision-makers seek a deeper understanding of how the cloud will fit within their organisations. While the cloud continues to generate a tremendous amount of attention, primarily due to the benefits it offers, only a handful of providers in the Kingdom currently provide cloud services. It is projected that in 2021, cloud spending in Saudi Arabia will reach $140 million. There should be a higher acceptance of cloud technologies despite an inherent desire among Saudi organisations to retain complete control over their IT functions.

3. INCREASING CYBER THREATS

In this section, we cover the cybersecurity challenges faced by Saudi Arabia. First, we attempt to identify the challenges by analysing the significant cyberattacks on the Kingdom's public sector.

With over 27 million consumers and a sizable number of global enterprises, Saudi Arabia is the largest Information and Communications Technology (ICT) market in the Middle East. The ICT strategy of the Ministry of Communications and Information Technology 2019-23 targets a goal of 50 per cent growth of the IT sector and raises the Saudi IT workforce to 50 per cent by 2023.

It also aims to attract foreign investments and support empowerment and more participation of women in the sector. The strategy is part of the government's efforts to establish a robust and cutting-edge digital architecture, so digital transformation accelerates and supports the Vision 2030 goal of promoting the sector's role to build a digital society, a digital government, a thriving digital economy, and innovation.

E-commerce, digital education, digital health, industry for intelligent cities, national data, and e-government are the primary beneficiary sectors of the ICT Strategy. The increased deployment of web and mobile applications by organisations is expected to lead to the growth of the cybersecurity market.

A need for expertise in cybersecurity is increasing with the growing sophistication of threats. The Kingdom of Saudi Arabia averagely faces 160,000 cyberattacks daily. The attacks are progressively proving catastrophic to the primary functions of the Kingdom by disrupting the critical services of both the governmental and the private sectors. Cyber-attacks of varying scales can result in severe damages to the economy and negatively impact the social and political stability of the country.

Given that cybersecurity is still a progressing domain in the Kingdom and is yet to attain maturity. As a result, the Kingdoms' ICT infrastructure remains vulnerable to a spectrum of cyber threats that many nation-states and non-state actors have tried to exploit.

Saudi Arabia and its strategic allies were frequently attacked by an Advanced Persistent Threat group (APT 33), a commotion of Middle Eastern hackers with a high level of sophisticated capabilities in espionage. The APT33 wreaked a substantial cyber-havoc spanning different USA, Saudi Arabia, and South Korea industries.

In 2017, APT33 targeted an ongoing Saudi- Korean conglomerate to mislead and entice the defence personnel through a spear-phishing.

Social media constitutes a vital mode of online communication environment. Wherein the users are authors of the contents and share and receive information in voluminous amounts. The information being shared on social media is available in heterogeneous formats such as blogs, forums, photo-sharing platforms, social gaming, chat apps, online social networks, etc. The social network penetration in Saudi Arabia appears to be compounding with 'WhatsApp' being the most preferred mode of communication and with a penetration rate of 73%.
The current trends indicate that terrorist's resort to social media as an alternative to ground operations to disrupt and impede the vital functions of a target nation and its economic activities. This can potentially lead to deaths, severe property damage and poising an extreme risk to the health and safety of the public, economic growth, political stability and cohesion of the country. The primary motives of Social Media Terrorism are to plan and share attack details, recruitment, propaganda and fundraising for terrorism activities.

4. CRIME AND SAFETY

Crime in Saudi Arabia has increased over recent years but remains at levels far below most major metropolitan areas globally. Criminal activity does not typically target foreigners and is primarily drug-related. The U.S. Department of State has assessed Saudi Arabia as being a HIGH-threat location for terrorism in 2020 [4].

Terrorists may attack with little - no warning. Terrorists have targeted Saudi and Western government interests, mosques, other religious sites (both Sunni and Shia), and some locations U.S. citizens and other Westerners frequent.

ISIS and al-Qa'ida in the Arabian Peninsula (AQAP) continue to demonstrate the ability to inspire individuals to conduct attacks and to expand operational capabilities for planning and executing attacks inside Saudi Arabia. Individual cells aligned with Shia militant groups also operate in Saudi Arabia. ISIS and AQAP have expressed their intent to continue attacks in Saudi Arabia. Multiple small-scale attacks have involved ISIS or ISIS-inspired assailants. In April 2019, armed terrorists attacked Saudi security forces in Qatif (Eastern Province) and Zulfi (160 km northwest of Riyadh). On November 11, 2019, a 33-year-old Yemeni male claiming affiliation with AQAP stabbed three cultural performers at a live show in Riyadh. In December 2019, Saudi security forces killed two terrorists possessing RDX explosives and materials for a car bomb in al Anud, a suburb of Dammam.

Authorities have conducted numerous arrests, identified smuggling routes, and interdicted attempts by ISIS and others to cross the border illegally. The government has a strong security force that has increased its ability to respond quickly anywhere in the Kingdom. However, the government struggles with confronting illegal immigration and smuggling along its southern border with Yemen. Saudi border guards reportedly have stopped thousands of people from crossing the border illegally and have encountered an increased volume of smuggled firearms and ammunition. The government is working on new initiatives to mitigate these threats, including fingerprinting passengers at airports and border crossings. The government has increased its use of media to announce arrests and request assistance from the populace in identifying and locating terrorists.

Iran and its regional proxies have attacked Saudi Arabia with missiles, rockets, and armed unmanned aerial systems (UAS). Iran and other regional actors hostile to Saudi Arabia have conducted destructive and sometimes lethal attacks against various targets, including critical infrastructure, military facilities, airports, and energy facilities throughout the country and merchant vessels in regional shipping lanes. Riyadh, Yanbu, areas in proximity to Jeddah, the civilian airport in Abha, military installations in the south, and specific oil and gas facilities are examples of recent targets. Iran has supplied Yemen-based Houthis and other regional proxy groups with weapons, including drones, missiles, and rockets. Violence associated with Iran and Iran-supported groups represents a significant threat. Citizens living and working near military bases and critical civilian infrastructure, particularly in the Eastern Province and areas near the border with Yemen, are at heightened risk of missile and drone attacks. Continuing violence in neighbouring countries, such as Yemen, can spill over into Saudi Arabia. The U.S. Government restricts government personnel and their families from travel to within 50 miles of the Saudi-Yemen border, including the cities of Jizan and Najran; al-Qatif in the Eastern province and its suburbs, including Awamiyah; and Abha International Airport (AHB).

Security forces generally do not tolerate public demonstrations and move quickly to prevent them from forming or gaining momentum. Drug use among Saudi youth is an increasing concern. Narcotics smuggling continues to be a challenge along with the border areas. The threat of kidnapping by terrorist groups continues despite recent counterterrorism efforts. Terrorist elements may resort to targeting individuals rather than carrying out large-scale attacks. Criminal kidnappings are usually associated with other violent crimes.

---

[1] https://www.statista.com/statistics/262742/countries-with-the-highest-military-spending/

[2] https://www.export.gov/apex/article2?id=Saudi-Arabia-Defense-and-Security

[3] https://www.arabnews.com/node/1697971/business-economy

[4] https://www.osac.gov/Country/SaudiArabia/Content/Detail/Report/f6af335c-d5b7-4087-9086-186575bdfb0f