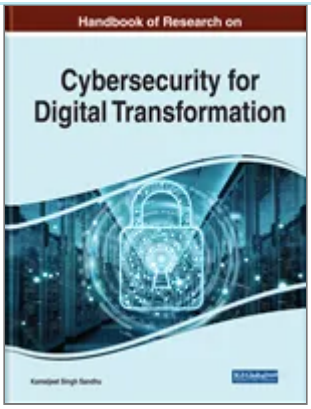

The Advancing Cybersecurity Ecosystem of Israel: An Overview of Current Challenges and Opportunities in the Early 2020s

Szabolcs Szolnoki (John von Neumann University, Kecskemét, Hungary) and Árpád Ferenc Papp-Váry (John von Neumann University, Kecskemét, Hungary)

Source Title: Handbook of Research on Advancing Cybersecurity for Digital Transformation (/book/handbook-research-advancing-cybersecurity-digital/258877)

Pages: 24

DOI: 10.4018/978-1-7998-6975-7.ch003

Abstract

True to its nickname 'cyber nation', the country of Israel is seen as a kind of role model in terms of intelligence and defence capabilities by many countries. The present study aims to provide a comprehensive but far from a complete picture of the cyber defence ecosystem of Israel, a country with more than 430 start-ups and unicorns valued at billions of US dollars. The authors outline the major incidents of the recent period, as well as current challenges and threats. The purpose of the chapter is to introduce good practices and cooperation for opportunities to policymakers and cybersecurity experts as well.

Chapter Preview

Top

Introduction: The Advancing Ecosystem Of The 'Cyber Nation'

The modern and independent State of Israel celebrated the seventieth anniversary of its proclamation of independence in 2018. Besides this landmark anniversary, the remarkable development of Israel's image in the past decade was also a cause for celebration. Nowadays, many people around the world consider Israel as a start-up nation, the stronghold of innovation, research and development and risk capital, and the home of outstanding researchers.

Israel is increasingly referred to as a 'Cyber Nation' as the country not only excels in defending its own cyberspace, but also 'exports' its capabilities. There is conscious country image building behind the brand name, which is not surprising as its aims are primarily economic, and their purpose is to develop competitiveness, for example, through the development of export (Papp-Váry, 2019). Government support for the cyber security industry has been present from the beginning with programmes such as Kidma[1] and Masad[2], which provide assistance for the sector's start-ups and facilitate a healthy competition between them. In addition, the government has partnered with the army, universities and the private sector. (Israel Cyber Alliance, 2021)

The cyber ecosystem boasts more than 430 companies, from listed large enterprises to start-up garage companies across the country. Their total value exceeds US$ 3.5 billion, representing about 5 percent of the global cyber security market. (Israel Cyber Alliance, 2021)

The most important current challenge is the shortage of manpower in the high-tech industry, which is also causing difficulties for government, academic and corporate actors in cyber security. In addition, considering all market participants, the fastest growing, innovative start-ups are threatened by the multinational companies' local research, development and innovation centres, enticing programmers and engineers with significantly higher salaries and extremely attractive fringe benefit packages. The average annual salary in the sector is NIS 275,714[3] (approximately USD 84 thousand). (Payscale, 2021) According to a 2019 survey by IVC Research Center, at least 800 highly skilled employees were needed in the sector employing approximately 20,500 people at the time of the study. (Solomon, 2019)

The list of challenges also includes the constant and intense threat not only in the physical space but also in cyberspace. Nevertheless, the country's reputation does not deter offensive political or economic rivals – on the contrary, the cyber cold war between Israel and Iran (which has been steadily intensifying for nearly a decade) has become more and more spectacular, making headlines in the world press with further attacks in 2020. From the beginning of the early 2010s, Iran started to invest significant financial resources in the development of its capabilities, both in technologies and training. Within a noticeably short period of time the country became a first-tier cyber power and a real threat to the top players of this game – the United States, Russia, China, and Israel according to cybersecurity experts and politicians. (Martins, 2018)

According to a recent report by US information security company F5 Labs, Israel became the number one target for hackers between July and October 2020, preceding the United States, India, Russia, Turkey and the Czech Republic. (Nocamels, 2020)

Key Terms in this Chapter

Cyber Attribution (/dictionary/cyber-attribution/100549): The process investigations to attribute the incident to specific threat actors in order to gain a complete picture of the attack, and to help ensure the attackers are brought to justice.

Phishing (/dictionary/phishing/22631): A phishing website is a site that presents itself as the official site of a known organization or company and attempts to obtain personal information, typically user IDs, passwords, and credit card information. Scammers often try to get users to click on the link in the message, which leads them to a phishing page by sending unsolicited emails and instant messages. If users follow the instructions there, they can become victims.

Botnet (/dictionary/botnet/37986): A botnet is a network of infected IT devices that can be used by a botnet host for multiple types of damage. The purpose of using infected workstations is primarily to send unsolicited mail, launch Denial-of-Service (DoS) attacks, or even steal sensitive (such as banking) data.

Ransomware (/dictionary/ransomware/24516): Blackmail (ransomware) is malicious software designed to "take hostage" in some way the data stored on users' IT devices, which it makes available again only upon payment of a ransom.

Malware (/dictionary/malware/17740): Software that is capable of copying itself while running an infected program. Depending on their prevalence, they can be viruses that infect files (such as macro viruses, executable infectious files, etc.) or viruses that infect the boot sector required to boot systems.

Spam (/dictionary/spam/27831): All bulk unsolicited messages sent electronically. These are most often created by so-called infected computers and distributed through robotic networks. The most common form is commercial e-mail sent to many addresses, promoting products or services that in many cases do not even exist. Spamming can take place through a variety of channels, such as SMS, instant messaging applications, social media, or voice messaging.

Denial-of-Service (/dictionary/denial-of-service/100550): Denial-of-service (DoS) attacks are electronic attacks that can load systems, services, or networks to such an extent that the affected system, service, or network may become inaccessible. This can be achieved on the one hand by paralyzing the systems and on the other hand by increasing the network traffic, as a result of which the legitimate data traffic does not reach the target system. A DoS attack can come from a single system or even a group of systems. The latter case is called Distributed Denial of Service (DDoS) attack.

Complete Chapter List