Noah Pineiro, Janeel Abrahams, Daniel Nunez

IDH3034

Professor Pestana

1 November 2020

Country Report

Cybersecurity is such an important thing nowadays. Without it, all of our information could be easily stolen and that would leave us as a huge disadvantage. Especially when it comes to military and government data, we cannot allow that type of information to be stolen. If used in the wrong hands, it could potentially mean the downfall of a country. For these reasons and more, cybersecurity is essential to today’s technological world.

Cybersecurity, (also known as computer security and information technology security), is “the practice of protecting systems, networks, and programs from digital attacks.” Usually, cyberattacks are aimed at “accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.” Today, we are going to be focusing on Israel and the power of its nation’s cybersecurity.

To start off, Israel is a Middle Eastern country found on the Mediterranean Sea. It has a population of a little under 9 million, and technology is one of Israel’s most developed sectors. Recently, Israel has been becoming “a cybersecurity powerhouse leading the $82 billion industry,” (Forbes, 2017). As it stands, Israel has one of the strongest military forces in the world. Compare that with their cybersecurity, and you could arguably say that they are on a whole other level. There are over “400 companies funded in the field of cybersecurity vs fewer than 1,000 in the United States despite being about 2% of the population. In fact, when Iran was hit in 2009 by a major computer virus that the US orchestrated, there were rumors that in fact it was Israel who carried out the mission on behalf of the United States,” (Rebellion Research, 2020). Clearly, Israel’s cybersecurity is not something to underestimate.

When it comes to cybersecurity, there are many forms that it can take; two of which we will be talking about. There is both offensive and defensive capabilities for cybersecurity. Beginning with the offensive track, this is when ethical (or in some cases, unethical) hacking is used to mimic a cyber-attack, break into a system to steal various data and information, etc. Offensive hacking is also referred to as taking a proactive approach to a situation. One of the most common types of offensive cybersecurity is a method known as pen-testing. This is when a simulated cyber-attack is created to evaluate the current security status of a business, organization, etc. Next up is the defensive track. This is when techniques are used to prevent cyber-attacks, data leaks, etc. This is also known as taking a reactive approach to cybersecurity. The main issue with defensive cybersecurity, however, is that not all defensive strategies are able to protect an organization from all threats.

Moving back to Israel, they have faced many cyberattacks, ranging from individuals to state hackers. This has cause Israel to have high defensive cybersecurity capabilities. In turn, Israel “has also been a leader in using the cyber realm for offense,” (International Studies Perspectives, 2015). One instance of this was Israel’s strike on Hamas hackers.

The aftermath of the Israel-Gaza fight caused 25 Palestinian and four Israeli deaths. What stood out most during this incident for cybersecurity professionals is that the Israeli Defense Force (IDF) “claimed that it bombed and partially destroyed one building in Gaza because it was allegedly the base of an active Hamas hacking group.” This was the “first true example of a physical attack being used as a real-time response to digital aggression,” (Wired, 2019). While the answer still remains unclear, the IDF had stated in a tweet that they “thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work. HamasCyberHQ.exe has been removed,” (Wired, 2019). After their successful cyber defensive operation, they were then able to (presumably) launch a counter offensive operation against the HamasCyberHQ. From there, they took to action via hybrid-warfare (a combination of conventional and cyberwarfare) and bombed the building in Gaza.

In terms of defensive capabilities, Israel definitely has that covered. “Since 2011, the Israeli government has worked to centralize and streamline cybersecurity authorities and responsibilities. It has established a new civilian national security agency—the National Cyber Directorate—to oversee cybersecurity preparedness in both the government and the private sector, and to monitor and respond to cyber threats,” (Hoover, 2020). The reforms that Israel was making were being extended only to domestic cyber defense.

A way that Israel is using both offensive and defensive cybersecurity is with a new collaboration with the United States. Currently, they have joined together to develop and advanced GPS anti-jam navigation system. This will allow further protection of essential assets, regardless of the platform. While this is being done, Israel is also working on creating “a weapon systems that can operate in GPS denied areas,” (Defence iQ, 2019). This is becoming more needed for the Israeli Airforce, seeing as how back in 2018 they performed over 200 air strikes to Iranian targets that were located in Syria. At the time, the area was always covered with GPS denying systems. If what they are currently working on is successful, then it would make those kinds of operations much easier, and safer to perform as well.

Overall, Israel’s technological advancements are very incredible. Having been ranked 5th in the world in technological innovations shows just how serious Israel is when it comes to technology, especially considering that, again, technology is one of Israel’s most developed sectors. In terms of cybersecurity, Israel ranks number two in taking cybersecurity deals. With their vast offensive capabilities and even stronger defensive capabilities, Israel’s cybersecurity is not to be messed with.

It would be of no surprise that such a technologically advanced country has implemented technology even into its political and cyber militia systems. As per implementing technology in the political systems the Israeli democratic party, Lukid uses an application called Elector to manage voter’s personal information. The application houses the full names, ID, and phone numbers, as well as their current addresses for all eligible voters in the country and it was leaked twice thus showing that even cyber powerhouses are not impenetrable. Even more concerning is the fact that the party continued to not only use that application, but they also began to endorse it after the first occurrence of information breach. Although the national Cyber Directorate and the Privacy Protection Authority were informed and took swift action, the mother company of the application also called Elector, ignored all evidence. Despite the many red flagged and concerns raised by the cybersecurity investigator Elector is still being used. The most recent update about this came from “Attorney General Avichai Mendelblit and the Privacy Protection Authority. Both of them argued that a petition to forbid Likud to use the app because of the information leaks from it should be rejected out of hand. They took this position even though the authority itself wrote in black on white that using Elector could still be dangerous, since an inquiry into it hasn’t yet been completed.” (Editorial,2020). Israel is high ranking in both cybersecurity thus making some of its highest values privacy and security however these are sidelined if they go against the political needs of the ruling party and the prime minister, Benjamin Netanyahu- this is evident to anyone who is closely following this scandal.

Similarly, as per the implementation of cyber militia technology, On May 9 2020 the usually bustling shipping traffic at the Shahid Rajaee Port came to a halt as officials reported that the port was a victim of a cyber-attack. According to an article published in the New York times “The attack on the computer systems at the Shahid Rajaee port in the strategically important Strait of Hormuz was limited in scope, creating traffic jams of delivery trucks and some delays in shipments, but causing no substantial or lasting damage.” Prior to Israel’s attack on the port both Iran and Israel have been in a back and forth rally of successful cyberattacks and Israel’s attack on the port was to make a statement to Tehran-“Don’t mess with Israel’s infrastructure.”(Bergman and Halbfinger,2020). The hacking of the port’s computers came in direct response, to a failed Iranian cyberattack on an Israeli water facility a month prior. Initially it was decided that the damage if the attempt were successful would have been minor enough to not matter so the Israeli officials decided to not retaliate, however, some government officials led by the defense minister who was serving his last days in that position seemed to prefer the law of retaliation “ עַ֚יִן תַּ֣חַת עַ֔יִן‎” (an eye for an eye”).

A pump had stopped working as a result of the Iranians’ attack on the Israeli’s municipal water systems in the Sharon region on April 24th  . A security company that investigated discovered that malware had caused the shutdown. In Israel water is a “critical infrastructure” as such the incident was reported to Israel National Cyber Directorate and other such intelligence agencies in Israel. According to Israeli officials , the cyber sector investigation unit identified the malware as coming from one of the offensive cyberunits of Iran’s Islamic Revolutionary Guards Corps.( (Bergman and Halbfinger,2020)

 Another interesting fact about this technologically innovative country is that before December 27, 2018 there was no actual laws in Israel governing the cyberspace and its uses. On that date the Knesset, Israel’s parliament passed an Amendment Law that gave a statutory basis to the unification of the Cyber National Bureau and the National Cyber Security Authority into the Israel National Cyber Directorate (INCD), which operates directly under the Prime Minister. The new law amended the Regulation of Security in Public Bodies Law, which regulates the protection of certain listed public bodies that provide essential public services, including computerized systems and information security. The mission, functions, and authority of the INCD were not yet regulated by the law. A Cyber Security and National Cyber Directorate Memorandum was published and distributed for public comments in July 2018 in anticipation of filing a cyber-protection bill for the approval of the Ministerial Committee for Legislation, and later consideration by the Knesset. The Memorandum seeks “to regulate the mission, functions and authority of the INCD to implement the government policy, in accordance with the principle of the rule of law, while combining basic concepts of constitutional law on subjects regulated under the draft bill and concepts of law and information technology.” According to the introduction of the Memorandum’s Summary, the objective of the INCD is to protect cyberspace and promote Israel as a global leader in the area of cyberspace. The functions of the INCD include managing the national defensive operational efforts against cyberattacks, promoting Israel’s ability to deal with cyberattacks, promoting international cooperation and cooperation agreements in the field of cyberspace, and advising the government and its cyber committees. The INCD will serve as “a dedicated body to deal with attacks before … [and] as they occur, without replacing other security and law enforcement bodies, but rather through interfacing with them.”(Levush,2019) This all ties back to he scandals with the Elector company as this law gives the Prime Minister complete control of the cyber regulations.

**Bibliography**

**https://www.threathunting.se/2020/06/25/defensive-offensive-cybersecurity/**

**https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html**

**https://www.rebellionresearch.com/blog/why-does-israel-dominate-cyber-security**

**https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-**

**powerhouse-leading-the-82-billion-industry/?sh=4a702ea420aa**

**https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/**

**https://www.hoover.org/sites/default/files/research/docs/chachko\_webready.pdf**

**https://www.defenceiq.com/cyber-defence-and-security/articles/how-israel-is-leading-the-global-**

Bergman, Ronen, and David Halbfinger. “Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks.” *The New York Times*, The New York Times, 20 May 2020, www.nytimes.com/2020/05/19/world/middleeast/israel-iran-cyberattacks.html.

Editorial, Haaretz. “Israel Has Failed to Address Severe Cybersecurity Issues, and Threats Are Imminent: Opinion.” *Haaretz.com*, Haaretz, 18 Feb. 2020, www.haaretz.com/opinion/editorial/israel-failed-to-address-severe-cybersecurity-issues-while-its-enemies-get-stronger-1.8552559?back=https%3A%2F%2Fwww.google.com%2Fsearch%3Fclient.

Levush, Ruth. “Global Legal Monitor.” *Israel: Knesset Passes Amendment Law Recognizing Role of National Cyber Directorate in Protecting Cyberspace | Global Legal Monitor*, 22 July 2019, www.loc.gov/law/foreign-news/article/israel-knesset-passes-amendment-law-recognizing-role-of-national-cyber-directorate-in-protecting-cyberspace/.

.