ISRAEL'S CYBER SECURITY ARCHITECTURE: A CASE STUDY

Dr Jatin Kumar
Researcher at Manohar Parrikar Institute for Defence Studies and Analyses.

Guncha Prakash
Independent researcher in the field of Public Policy and Geo-economics and has done her Masters in Economics from University of Warwick, United Kingdom.

The modern system of warfare is no more limited to the traditional tangible threats such as border skirmishes and military combats. The state and non-state actors have started actively exploiting the intangible domain of cyber space to pose security threats which are characterised by anonymity and boundlessness. Countries are competing to upgrade their technological knowhow and feed manipulated information to their enemies to direct it into fulfilling the former's interests, as has been seen in the alleged intervention of countries in elections of others to dictate the outcomes of the polls. Thus, cyber warfare, by following the principle of 'minimum intervention, maximum damage', has increased the vulnerabilities and insecurities of the world players and has additionally created an environment wherein countries are willing to outcompete each other to reach unpeaceful ends.

A country that is recognised as a significant player in the cyber domain is Israel. Despite COVID 19 crisis, its cyber industry displayed a positive growth trend in 2020, with a 70 percent increase in the amount raised (a record USD 2.9 Billion) from over 100 different deals, as compared to the previous year[1]. It has developed a robust cyber infrastructure and has made great strides in science and technology developments and cybersecurity solutions as a result of the various hostilities it has faced from its surroundings over time. It is surrounded by Arab nations on all sides with their relations being termed as 'cold peace'. A very small human resource base (around 9 million) in comparison to the Arab forces further adds to its insecurities. The Iranian presence in Syria, Lebanon, Iraq and Yemen has also proved to be a major force to reckon with.

In addition to the above, the heavy reliance of Israel's economy on information and operational technology, has exposed it to a multitude of cyber risks. All the above have compelled Israel to achieve technological superiority, supremacy in cyber surveillance and cyberwarfare to effectively confront its adversaries and protect its economic establishments.

The rapid expansion in cyber domain in mid-2000s and high-profile cyber breaches in 2010s made it necessary for Israel to make substantial investments in its cybersecurity organisations starting with establishment of National Cyber Bureau (2012) to the formation of Israel National Cyber

Directorate in 2016. Apart from catering to its national security requirements, it has also recognised the importance of using cyber domain knowledge as a business opportunity. This was reflected in Prime Minister Benjamin Netanyahu's speech at Tel-Aviv University's 7th Annual Cybersecurity Conference. At the conference, he said "cyber is a great business. It's growing geometrically because there is never a permanent solution, it's a never-ending business"[2].

Role of Government Agencies in Cyber Security

In Israel, the role of the government in developing and sustaining the cyber domain and technology sector is remarkably significant. There is consensus among the scholars that IDF has proved to be a breeding ground for Israel's defensive and offensive cyber capabilities. There exist special intelligence units of the IDF, namely Unit 8200 and Unit 9900, which provide young IDF soldiers practical experience in dealing with cybersecurity challenges and solutions[3]. Many cyber experts in Israel have effectively honed their technological skills in these units, which through their start-up-like functioning provide recruits the necessary exposure and understanding to work in a team-oriented environment.

Apart from equipping the military to deal with cyber threats, Israel has also developed a robust mechanism to counter the cyber based challenges in the civilian sphere. The Israel National Cyber Directorate (INCD) formulates policies and builds technological capabilities to defend cyberspace. INCD is also in charge of establishing and reinforcing "the cyber science-and-technology base by developing high quality human capital, supporting advanced academic research, engaging in deep technological R&D and fostering the cyber industry"[4].

Israel and Cyberwar

Since 1948, Israel has confronted various types of attacks (conventional and non-conventional) from its hostile Arab neighbours. Although, in the last decade, it has successfully neutralized many attempts at infiltration in its cyberspace, there are growing concerns that its adversaries will be able to narrow down the technological gap to challenge its existing superiority.

The various cyber-attacks faced by Israel, especially over the last one decade have posed serious challenges for its national security agencies and the economy as a whole. Some significant examples of the same are mentioned henceforth. In 2013, an anonymous group of hackers targeted the website of an Israeli NGO that assists children suffering from cancer[5]. Since 2013, it has been dealing with an annual cyber-attack, known as OpIsrael which has targeted government and corporate websites on an annual basis. In August 2018, Iranian hackers "Leafminer" targeted Israel and other Arab Countries, Saudi Arabia, the UAE, Qatar, Kuwait, Bahrain and Egypt[6]. In April 2020, Iran allegedly targeted Israel's water infrastructure facilities, which was also allegedly retaliated by Israeli counter attack on Iran's busiest hub for maritime trade, Shahid Rajaee Port in Bandar Abbas on May 9, 2020[7]. On December 18, 2020 a major cyberattack halted various Israeli logistic companies.

To deal with such cyber-attacks, Israel has developed offensive and defensive capabilities by encouraging and institutionalising educational and technological mechanisms, in the form of courses on cybersecurity and extensive research endeavours in the cyber realm. At offensive level, it developed know-how to use cyberspace as a weapon to confront its adversaries[8]. For instance, in 2010, the US-Israel together targeted the Iranian nuclear programme with the Stuxnet virus[9]. Both had reportedly also worked together to hit the Iranian nuclear program with the Flame virus[10]. In Syria, it reportedly used cyber tools to support IDF's operations while targeting Syrian nuclear reactors. During the attack it hacked Syrian radars and reprogrammed them, projecting Syrians that everything was fine while strikes were underway[11]. In 2019, an Israeli Company (NSO Group) targeted a group of Whatsapp users (Palestinian and Iranian) with surveillance software which was capable enough to get information from both iPhones and Android[12].

At a defensive level, Israel has constantly been advancing its technological knowledge in the cyber domain and timely upgrading its weapons and communication system that might be vulnerable to cyberattacks. The responsibility to protect the military communication system is on the shoulders of C4I Branch of IDF while the INCD is responsible for protecting the civilian cyber sphere. In addition, the cyber capabilities of Intelligence agencies such as Mossad are further aiding Israel's cyber war efforts against its enemies.

Apart from setting up internal institutional mechanisms, Israel has also partnered with various countries to collaboratively defend cyberspace. For example, in July 2014, Israel and Japan signed an agreement providing funds to Israeli and Japanese companies for joint research in areas of cybersecurity[13]. In 2017, a US-Israel Cyber Working Group was established to advance cooperation on cybersecurity[14]. Similarly, in January 2018, India and Israel signed an MoU on Cyber Security Cooperation during Prime Minister Benjamin Netanyahu's visit to India[15]. To deal with the rising cyber threat amid rapid digitisation during COVID 19 crisis, Director-General of Israel's National Cyber Directorate (INCD), Yigal Unna, and Indian Ambassador to Israel, Sanjeev Singla signed another MoU (July16, 2020) to expand the cyber ties between the two countries[16]. Such bilateral endeavours to tackle the problem of cybersecurity hold great promise in the future.

Conclusion

With cyber security threats in the form of cyber terrorism, malware and ransomware attacks on strategic and non-

strategic infrastructure and data hijacking, looming on the heads of every single nation of the world, the need to address these is being felt more than ever. With Israel leading in cybersecurity, its indispensability in aiding the world cannot be ignored.

The various internal and external threats have strengthened Israel's cybersecurity architecture in the form of establishment of robust institutions over time such as units within IDF and INCD. Furthermore, the various Israeli business start-ups in Israel are also actively developing new age solutions in the cyber domain. Hence, Israel can benefit the global community through active knowledge sharing and technical training initiatives.

With regards to India, deepening Indo-Israeli cooperation in the cyber domain will indeed help in setting up a sustainable cyber ecosystem. These areas of cooperation may span from regular academic engagements such as introduction of educational and vocational courses involving student and employee exchanges to frequent seminars by cyber professionals in government and private institutions. Furthermore, there can be collaborations between start-ups from the two countries and channels of real time information sharing can be instated. All of these will ensure that both countries reap mutual benefits of information and knowledge sharing in the cyber domain.

References

1. *Israel National Cyber Directorate, "The Israeli cyber industry continues to grow: record fundraising in 2020", https://www.gov.il/en/departments/news/2020ind*

2. *Gil Press, "6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry ", https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/?sh=6ee4b0ab420a*

3. *Ibid.*

4. *Israel National Cyber Directorate, https://www.gov.il/en/departments/about/newabout*

5. *The Guardian, "Anonymous hacker attack on Israeli websites 'causes little real damage" https://www.theguardian.com/technology/2013/apr/08/anonymous-hacker-attack-israeli-websites*

6. *Sandeep Singh Grewal, "Report: Iran hacks Israel in cyber-attack" https://www.jpost.com/israel-news/politics-and-diplomacy/report-iran-targeted-israel-in-cyber-attack-563937*

7. *Gil Baram and Kevjn Lim, "Israel and Iran Just Showed Us the Future of Cyberwar with Their Unusual Attacks", https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/*

8. *Cohen, Matthew & Freilich, Charles & Siboni, Gabi. (2016). Israel and Cyberspace: Unique Threat and Response. International Studies Perspectives. 17. 307-321. 10.1093/isp/ekv023.*

9. *Stuart Winer, " 'Dutch mole' planted Stuxnet virus in Iran nuclear site on behalf of CIA, Mossad", https://www.timesofisrael.com/dutch-mole-planted-infamous-stuxnet-virus-in-iran-nuclear-site-report/#:~:text=The%20Stuxnet%20virus%20was%20uncovered,by%20speeding%20up%20its%20centrifuges*

10. *Reuters, "Israel developed Flame computer virus: newspaper", https://www.reuters.com/article/net-us-usa-cyber-flame-idUSBRE85I1QQ20120619U.S.*

11. *Cohen, Matthew & Freilich, Charles & Siboni, Gabi. (2016). Israel and Cyberspace: Unique Threat and Response. International Studies Perspectives. 17. 307-321. 10.1093/isp/ekv023.*

12. *The Financial Times, "WhatsApp voice calls used to inject Israeli spyware on phones", https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab*

13. *Franz-Stefan Gady, "Japan and Israel to Work Together in Cyberspace" , https://thediplomat.com/2015/01/japan-and-israel-to-work-together-in-cyberspace/*

14. *Josh Kram, "US-Israel Cybersecurity Collaborative: A Roadmap for Global Private, Public Partnership", https://www.uschamber.com/series/above-the-fold/us-israel-cybersecurity-collaborative-roadmap-global-private-public*

15. *Ministry of External Affairs, "List of MoUs/Agreements signed during the visit of Prime Minister of Israel to India (January 15, 2018)", https://mea.gov.in/bilateral-documents.htm?dtl/29356/List_of_MoUsAgreements_signed_during_the_visit_of_Prime_Minister_of_Israel_to_India_January_15_2018*

16. *Press Trust of India, "India and Israel sign agreement to expand cooperation in cyber security" (Published in Hindu), https://www.thehindu.com/news/national/india-and-israel-sign-agreement-to-expand-cooperation-in-cyber-security/article32102730.ece*