MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

Israel's Approach to Building Cyber Capabilities: Lessons for the Indian Armed Forces

Guriqbal Singh Gill

May 31, 2023

Summary

India's 2013 National Cyber Security Policy (NCSP) aimed to produce 500,000 cybersecurity specialists by 2018. According to estimates, there are currently only about 150,000 of these specialists. In order to develop effective cyber capabilities, the Indian armed forces in particular could study the whole-of-nation approach of countries like Israel and their cyber talent development programmes, which have ensured a steady stream of cyber professionals, catering to that country's requirements of ensuring effective defensive and offensive cyber capability.

Introduction

Governments around the world have been concerned about the dangers of cyberspace for more than two decades. Until the turn of the century, it was rare to find academics and practitioners who claimed that cyber warfare was more than just a means of assisting kinetic multi-domain conflict in the physical domain.[1] With the creation of the US Cyber Command in 2010, China's relentless pursuit of information domain dominance with its own Strategic Support Force (SSF), and most recently, Russia displaying an increasing level of maturity in the field as evidenced by the success of its cyber campaigns in Estonia, Georgia, and Ukraine, the situation is drastically different.[2]

Dangerous cyberspace operations are currently being combated in a concerted and ongoing effort. National cyber security and cyber defence policies and plans have been developed and are being implemented by governments all over the world.[3] India's National Cyber Security Policy (NCSP) was published in 2013. Almost every facet of cyber security is covered in this extremely comprehensive write-up.[4] Further on, in 2019, the government also gave its approval for the creation of a Defence Cyber Agency (DCyA).[5]

One does not have to be an expert to conclude that the identification, development/training, utilisation, and sustainment of adequately trained cyber specialists will be crucial for the Indian armed forces' capacity building of cyber power. When it comes to the employment of cyber power, the operator is the 'man behind the gun', hence his skill set is crucial. Additionally, India needs cyber commanders who are capable of organising and executing cyber operations in both standalone and integrated application, in conjunction with Information Warfare and kinetic power, at both the tactical and strategic levels.

By 2018, the NCSP-2013 aimed to produce 500,000 cybersecurity specialists. There are currently only 150,000 of these specialists, according to estimates. In order to cater to the needs of developing effective cyber capabilities, there is an additional requirement for 500,000 professionals with the relevant skills.

Therefore, a comprehensive recruitment strategy must be put in place. Our sociology and human resource policies need to be adjusted to take into account this new

[1] Lt. Gen. R.S. Panwar, **"Towards an Effective and Viable Information Warfare Structure for the Indian Armed Forces"**, USI, 2018.

[2] Michael Connell and Sarah Vogler, **"Russia's Approach to Cyber Warfare"**, *CNA*,2017.

[3] Eric Luiijf, Kim Besseling, and Patrick De Graaf, **"Nineteen national cyber security strategies"**, *International Journal of Critical Infrastructures*, Vol. No.9, Issue No. 1/2 , 2013, pp. 3–31.

[4] **"National Cyber Security Policy -2013"**, MeitY, 2013.

[5] **"India set to get Defence Cyber Agency to fight Pak, Chinese hackers"**, *ANI,* 30 April 2019.

generation of cyber-warriors. This may include adapting already-existing educational and training programs or perhaps creating entirely new ones, as well as altering hiring procedures. The issue of retaining and enlisting Cyber Warriors is one that concerns nations all around the world.[6]

The Israeli Defence Forces (IDF) have excelled in building robust cyber capabilities, primarily due to their systematic development of talents through a whole-of-nation approach. This Brief will explore the IDF's approach to building cyber capabilities, with a focus on talent development and the whole-of-nation approach to talent scouting through various programs, and aims to draw lessons for the Indian armed forces.

Israel's Cyber Challenges and the Development of Capabilities

Israel, due to its unique geopolitical situation, faces a myriad of security challenges that require constant vigilance and advanced defence mechanisms. Surrounded by hostile neighbours and confronted with ongoing regional conflicts, the country has become a prime target for cyber threats. In response to these challenges, Israel recognized the critical importance of bolstering its cyber defences and actively engaging in cyber warfare capabilities.[7] The Israeli Defence Forces (IDF), in close collaboration with intelligence agencies, have played a pivotal role in the development of these capabilities.

Like India, the cyber threats faced by Israel are diverse and multifaceted. They range from state-sponsored attacks to those orchestrated by terrorist organizations and hacktivist groups. Hostile neighbouring countries, which reject Israel's existence, continuously seek ways to exploit vulnerabilities in its critical infrastructure and military networks. These countries aim to disrupt essential services, compromise national security, and gain unauthorized access to sensitive information. The ever-evolving nature of cyber threats necessitates a comprehensive and proactive approach to safeguarding Israel's digital landscape.[8]

To address these challenges, the IDF has made significant strides in developing robust cyber defence capabilities. The focus lies in building resilient networks, securing critical infrastructure, and establishing early warning systems to detect and

[6] Mark Townsend, **"Inside the British military base where young hackers learn to stop cybercrime"**, *The Guardian*, 19 August 2018.

[7] Jasper Frei, **"Israel's National Cybersecurity and Cyberdefense Posture: Policy and Organizations"**, Centre for Security Studies, September 2020.

[8] Matthew S. Cohen, Charles D. Freilich, & Gabi Siboni, **"Israel and Cyberspace: Unique Threat and Response"**, *International Studies Perspectives*, Vol. No. 17, Issue No.3, 2015, pp. 307–321.

mitigate cyber threats promptly. The IDF invests in cutting-edge technologies, conducts rigorous threat intelligence analysis, and maintains a highly skilled cyber workforce to stay ahead of emerging threats.

In addition to defensive measures, Israel has recognized the importance of proactive offensive strategies to deter potential adversaries and disrupt their cyber capabilities. The IDF, in collaboration with intelligence agencies, has developed offensive cyber warfare capabilities to counter cyber threats at their source. These capabilities enable Israel to identify, track, and neutralize potential cyber threats before they can cause significant harm.

The IDF's approach to cyber warfare combines advanced technological capabilities with intelligence-driven operations. By integrating cyber intelligence with traditional military operations, Israel is able to gather vital information, exploit adversary vulnerabilities, and execute precision-targeted cyber operations. These operations serve as a deterrent, sending a clear message that any cyber aggression against Israel will be met with a robust response.[9]

The development of Israel's cyber capabilities serves as a valuable lesson for other nations, including India, in addressing the challenges posed by the evolving cyber threat landscape. A comprehensive and multi-faceted approach that combines defensive measures, intelligence analysis, proactive offensive strategies, and continuous investment in talent and technology is crucial to building effective cyber defences.

Achievements in the Realm of Offensive Cyber Warfare

Successes in defensive cyber operations are difficult to quantify and often go unnoticed. However, a look at Israel's offensive cyber operations is pertinent. The IDF have made significant achievements in the realm of offensive cyber warfare, showcasing their expertise and capabilities in conducting offensive cyber operations.

Operation Orchard was an airstrike conducted by the IDF in 2007, targeting a suspected Syrian nuclear reactor. Prior to the physical attack, the IDF reportedly launched a cyber campaign aimed at disrupting Syrian air defence systems, effectively neutralizing their ability to respond to the impending airstrike. This operation showcased the IDF's integration of offensive cyber capabilities into conventional military operations.[10]

[9] Lior Tabansky, **"Israel Defense Forces and National Cyber Defense"**, *Connections*, Vol. No.19, Issue No.1, 2020, pp. 45–62.

[10] **"Operation Orchard/Outside the Box"**, International Cyber Law: Interactive Toolkit, 2007.

One of the most well-known and widely-discussed examples of offensive cyber warfare is 'Stuxnet', which targeted Iran's nuclear facilities. Although the involvement of the IDF has not been officially confirmed, reports suggest that Israeli intelligence, in collaboration with the United States, developed and deployed the Stuxnet malware. This operation successfully disrupted Iran's uranium enrichment program, causing significant setbacks to their nuclear ambitions.[11]

Subsequently, during the 2014 conflict between Israel and Hamas, the IDF incorporated offensive cyber operations as part of their overall military strategy. The IDF targeted Hamas' communication networks, command and control systems, and other infrastructure to disrupt their capabilities and undermine their operational effectiveness. Offensive cyber operations played a crucial role in degrading Hamas' ability to coordinate and carry out attacks.[12]

These achievements highlight the IDF's proficiency in offensive cyber warfare and their ability to leverage cyber capabilities to achieve strategic objectives. Israel's success in the field of cyber warfare can be attributed to several key contributions. First and foremost, Israel has a strong emphasis on technological innovation and boasts a vibrant Start-Up culture, which has fostered the development of cutting-edge cybersecurity solutions. Collaboration between the military, academia, and industry has played a crucial role, allowing for knowledge sharing and the rapid implementation of new technologies.

Additionally, the IDF places great importance on cyber skills and has invested heavily in training and recruiting talented individuals with exceptional technical skills. Israel's intelligence agencies, such as Unit 8200, have served as talent pools, producing a skilled workforce experienced in cyber operations. Lastly, the nation's proactive approach to cybersecurity, including proactive defence strategies, information sharing, and international cooperation, has helped Israel stay ahead of emerging threats and maintain its position as a global leader in cyber warfare. There is a special need to study Israeli cyber talent development programs in view of India's human resource development challenges in the cyber domain.

Israeli Cyber Talent Development Programs

It is evident that Israel has gained global recognition for its robust cyber warfare capabilities. A significant part of its success can be attributed to its talent development programs that are serving as an assembly line for extremely talented and diverse cyber warriors. These programs play a vital role in identifying, nurturing,

[11] Josh Fruhlinger, **"Stuxnet explained: The first known cyberweapon"**, *CSO*, 31 August 2022.
[12] No.8

and developing exceptional cyber talents from an early stage. Among the notable programs are Magshimim, Atudai, Mofet, Mamriot, Odyssey, and Gsharin. There is a need to further explore these programs to identify lessons in the Indian context.

Magshimim is a prestigious high school program in Israel that focuses on cybersecurity education. It aims to identify talented students with a passion for technology and cybersecurity and provide them with specialized training and mentorship. The program offers a unique curriculum that includes in-depth courses in computer science, cryptography, and network security. Magshimim nurtures students' interest in cybersecurity, equipping them with the necessary skills and knowledge to excel in the field. Graduates of Magshimim often pursue careers in cybersecurity, including joining the IDF's elite cyber units.[13]

Atudai is an academic scholarship program that supports exceptional students pursuing cybersecurity-related degrees at universities and colleges in Israel. The program offers financial support to talented individuals, enabling them to focus on their studies without the burden of financial constraints. Atudai scholars are selected based on their academic achievements, commitment to cybersecurity, and potential to contribute significantly to the field. The program not only provides financial assistance but also facilitates networking opportunities, mentorship, and access to industry experts. It aims to attract and retain talented individuals in the cybersecurity domain, bolstering the nation's cyber capabilities.[14]

Mofet or 'Cyber Girls' is a talent development program specifically designed for women in cybersecurity. Recognizing the importance of gender diversity in the field, Mofet encourages and supports women to pursue careers in cybersecurity. The program provides specialized training, mentorship, and networking opportunities, empowering women to excel in the male-dominated cybersecurity industry. By breaking down barriers and promoting gender equality, Mofet contributes to the development of a diverse and inclusive cybersecurity workforce.[15]

Mamriot is a similar program that focuses on training cyber defenders for critical infrastructure protection. It identifies talented individuals with a specific interest in safeguarding critical systems and provides them with specialized training in areas such as industrial control systems (ICS) security, network protection, and incident response. Mamriot equips participants with the skills and knowledge required to defend critical infrastructure against cyber threats, ensuring the resilience of essential services.

---

[13] Josephine Wolff, **"Making a new Pipeline"**, *Slate,* 6 July 2016.

[14] **"Atudai Program"** Jerusalem College of Technology.

[15] Larry Luxner, **"This new program is recruiting Israeli girls for cyber warfare and high-tech futures"**, *Jewish Telegraphic Agency*, 2018.

Odyssey is an initiative that aims to foster collaboration between the IDF and academic institutions in the field of cybersecurity. Under this program, selected students from universities engage in research projects and work alongside IDF cyber units. This collaboration promotes knowledge exchange, allows students to gain real-world experience in cybersecurity operations, and facilitates the development of innovative solutions to emerging cyber challenges. Odyssey bridges the gap between academia and the military, ensuring a continuous flow of talent, research, and expertise.[16]

Gsharin is a talent development program that focuses on attracting and nurturing individuals with a unique aptitude for cybersecurity. It targets individuals from diverse backgrounds, including those without traditional academic qualifications from various communities including Arabs and Druze. Gsharin seeks individuals with exceptional problem-solving skills, creativity, and a deep understanding of technology. Through specialized training and mentorship, Gsharin prepares participants for various roles in the cybersecurity industry, contributing to the development of a highly skilled and diverse cyber workforce.

Conclusion

These talent development programs demonstrate Israel's commitment to nurturing cyber talents and developing a strong pipeline of skilled professionals. By focusing on early education, academic scholarships, specialized training, and collaboration, these programs contribute to the nation's overall cyber capabilities. The success of these initiatives lies in their ability to identify exceptional individuals, provide them with targeted support, and create an ecosystem that fosters innovation and collaboration.

The Indian armed forces can draw valuable lessons from these Israeli talent development programs. By implementing similar initiatives, India can identify and nurture exceptional cyber talents, bridge the skills gap, and build a robust defence cyber workforce. Programs like Magshimim and Atudai can be adapted to the Indian context to attract talented students and provide them with the necessary resources and mentorship. Collaborative initiatives, such as Odyssey, can facilitate partnerships between academia and the military, fostering innovation and knowledge exchange. The Indian armed forces can tailor similar programs to strengthen their own defence cyber capabilities, address skill shortages, and foster innovation in the field of cybersecurity.

[16] Bharti Jain, **"Israel focuses on training next-gen to drive its cyber systems"**, *The Times of India*, 6 July 2022.

About the Author

Col. Guriqbal Singh Gill is Research Fellow at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses