RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 192 – 2 October 2014

Building a Cyber Iron Dome: Israel's Cyber Defensive Envelope

By Michael Raska

Synopsis

Israel is developing "a national cyber defensive envelope" – a multi-layered cyber defence strategy leveraging automated computerised systems and highly-trained personnel that provide intelligence, early warning, passive and active defence, and offensive capabilities across civil-military networks.

Commentary

ISRAEL'S SECURITY establishment is currently debating the political and military assessments and lessons of the war in the Gaza Strip in July-August 2014, known as 'Operation Protective Edge'. There is a consensus on the widening spectrum and increasing sophistication of cyber threats. During the conflict, Israel faced large-scale cyber-attacks on its civilian communications infrastructure, including denial of service (DDoS) and Domain Network System (DNS) attacks from both state and non-state actors, traced to Qatar and Iran - Hamas' main benefactors.

Cyber attackers also targeted the Israel Defence Forces (IDF) – its websites and communications networks. The Israeli Security Agency (Shin Bet) announced that these attacks against government and military networks had been contained, while in the civilian sector the attacker's intent to cause maximum disruption was not achieved. Still, cyberattacks – as projected by Prime Minister Benjamin Netanyahu – are viewed as "one of the four main threats to Israel."

Israel's Evolving Cyber Defence Strategy

While Israel has not published official cyber defence strategy, an analysis of Israeli cyber debates and leading open forums such as the Annual Cyber Security International Conference organized by the Yuval Ne'eman Workshop for Science, Technology and Security at Tel Aviv University, yielded four underlying drivers: (1) leadership support for a national cyber defence vision; (2) continuous upgrading of IDF's cyber defence capabilities such as in the Unit 8200; (3) Israel's cutting-edge R&D programs for boosting civilian and dual-use cyber capabilities; and (4) the development of a unique comprehensive national "cyber eco-system."

At the highest levels, Israel's cyber defence policy has been led by the Prime Minister's Bureau, which established a National Cyber Bureau (NCB) in August 2011. The NCB has brought a new

interdisciplinary thrust into Israel's cyber security, aiming to link civil-military expertise to tackle evolving cyber threats.

Paradoxically, the NCB has been opposed by Shin Bet, the internal security agency, which argued that action against hackers should be taken proactively in the early organisation and planning stages, rather than reactively. The Shin Bet claimed that the NCB is unable to carry out this task because it lacks intelligence-gathering capabilities, has no operational tradition of deterrence and no possibility of integration with similar security organisations worldwide.

After nearly two years of policy battles, Prime Minister Netanyahu announced on September 21 the establishment of a new government authority alongside the NCB with the responsibility for protecting Israel's economy and civilian space from computer attacks; effectively rejecting recommendations of the Shin Bet security services.

Meanwhile in the military domain, the IDF has been consistently upgrading its cyber capabilities and network defences. Well-known units of the IDF that specialise in various aspects of computer network operations are frequently profiled in the media for their high levels of operational sophistication, technological advances, and training. These include the Intelligence Corps Unit 8200 tasked with signal intelligence (SIGINT) and code decryption; the Cyber Unit within 8200, established in 2009; the C4I Branch developing netcentric warfare concepts and technologies; and other intelligence units. In 2013, the IDF also established a new Cyber Branch tasked to integrate operational concepts based on strategic needs and cyber capabilities of the IDF.

The experiences, training, and expertise of many former IDF Unit 8200 members have over time diffused into Israel's cutting-edge high-tech R&D sector, reinforced by the "start-up nation" culture. As of 2014, there are over 200 Israeli start-ups working on innovative cyber security solutions, resulting in US$3 billion in cyber exports, second only to the United States worldwide and constituting 5% of the global market, according to the National Cyber Bureau. Moreover, in 2013 Israeli start-ups raised US$165 million in investment funding, a figure which represents 11 percent of global capital invested in the field of cyber security. According to the NCB, 14.5 percent of all the firms worldwide attracting cyber-related investment are Israeli-owned.

In this context, Israel is creating a unique, symbiotic national "cyber eco-system." Strategic cooperation among leading national sectors: the defence establishment, private enterprise, academia, and key government agencies such as the Chief Scientist and the Ministry of Defense's Export Controls Agency shape national cyber security priorities, and more importantly, the implementation of cyber security innovation across civil-military domains.

Israel's Cyber Iron Dome

During the Operation Protective Edge, the main defence system used by Israel against the rocket attacks was the Iron Dome system operated by the Israel Air Force. The system is composed of a locator-radar, which identifies the rocket's source and tracks its trajectory, launcher with advanced interceptor missiles (Tamir), and a command and control centre which calculates the likely target. Iron Dome effectively creates a defensive envelope around a specific area, and is able to launch selective salvo intercepts against multiple incoming rockets with a success rate of 90%.

As of now, one of the influential schools of thought in the Israeli cyber debate is discussing the applicability of the operational concepts and lessons learned from the Iron Dome missile defence methodology in the cyber domain. For example, how to create effective cyber intelligence (enemy analysis & target creation), early warning and absorption readiness, strike effort, area suppression, active defence, command and control, passive detection, and ultimately, cyber deterrence.

Israel's cyber innovation must therefore be linked to the changing strategic realities over the past decade, including the emergence of the varying cyber threats that have created yet another layer of asymmetric security predicaments, while mitigating the effectiveness of Israel's traditional deterrence, early warning, and rapid military decision strategies. Amid these changes, Israel's subconventional threat spectrum has blurred the traditional offence and defence lines and widened the scope and character of operational requirements, including the need to protect both the physical and cyberdomains concurrently.

Michael Raska is a Research Fellow at the Institute of Defence and Strategic Studies, a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University in Singapore.

Nanyang Technological University
Block S4, Level B4, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg