CONFRONTING CYBERSECURITY CHALLENGES:

ISRAEL'S EVOLVING CYBER DEFENCE STRATEGY

Policy Report
January 2015

Michael Raska

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

Policy Report

CONFRONTING CYBERSECURITY CHALLENGES: ISRAEL'S EVOLVING CYBER DEFENCE STRATEGY

Michael Raska
January 2015

Military Transformations Programme,
Institute of Defence and Strategic Studies (IDSS),
S. Rajaratnam School of International Studies (RSIS),
Nanyang Technological University (NTU),
Singapore

Executive Summary

While Israel has not yet published a national cyber defence strategy, an analysis of the trajectory of Israeli cyber issues, policies and debates yields four key pillars: (i) support for a national cyber defence vision at the highest levels of national leadership; (ii) continuous upgrade of IDF's cyber defensive and offensive capabilities such as in the Unit 8200; (iii) Israel's cutting-edge R&D programmes for boosting civilian and dual-use cyber capabilities; and (iv) the development of a unique comprehensive national "cyber eco-system." In the process, Israel is developing "a national cyber defensive envelope"—a basis for multi-layered cyber defence strategy leveraging an innovative multi-stakeholder approach that combines intelligence, early warning, passive and active defence, and offensive capabilities across civil-military domains. In this context, "cyber" debate within and outside the Israeli defence establishment has shifted towards the emerging threats, challenges as well as opportunities of cyberspace as a new medium for civil-military strategic interactions.

Acknowledgements

In August 2014, the author of this report attended the fourth Annual Cyber Security International Conference, organised by the Yuval Ne'eman Workshop for Science, Technology, and Security at Tel Aviv University. This engaging and dynamic conference allowed the author to conduct further interviews with leading Israeli cyber experts, strategic thinkers, and practitioners in the academic, government, military and private sector arenas. While many wish to remain anonymous, special thanks goes to Ram Levi, Dima Adamsky, Isaac Ben-Israel, Daniel Cohen, Deborah Housen-Couriel, Rami Efrati, Ehud Eiran, Amos Granit, Yaniv Harel, Ofir Hason, Ilan Mizrahi, Iddo Moed, Deganit Paikowsky, Gabi Siboni, and Lior Tabansky. The author would also like to thank Arnon Eshel, Amir Horkin, Iris and Meytal Nasie.

Cyber Threats in Israel's Asymmetric Conflict Spectrum

Since the end of the Yom Kippur War in 1973, Israel's strategic environment has been increasingly characterised by the convergence of more complex "supra" and "sub-conventional" or hybrid security threats.[1] These have gradually combined conventional, asymmetrical, low-intensity and non-linear threat dimensions, and included regional proliferation of weapons of mass destruction (WMD) and ballistic missiles, low-intensity conflicts and terrorism, traditional security threats posed by potential conventional power projection aspirations by neighbouring states, and more recently cyber threats. The increasing amalgamation of security threats have in turn created greater security uncertainties and defence policy challenges, which have propelled robust debates in Israel's strategic and policy communities regarding the relevance of traditional security paradigms, direction and scope of particular force modernisation programmes, and overall strategic choices.

In the process, the task of formulating a comprehensive strategic blueprint of what constitutes "new ways of war" has proven challenging. Security planners in Israel must answer anew to what degree are their established defence planning methods relevant in meeting the continuing conventional security threats as well as a wide spectrum of emerging conflicts and non-linear crises? How to resolve the gap between long-term strategic planning and short-term operational requirements? What weapons technologies and systems should be procured at what price, and which of them are relevant within an affordable framework? And perhaps most importantly, how to build, train and maintain an organisational force structure capable of dealing simultaneously with current security threats while anticipating future challenges in the era of increasing strategic uncertainty and operational complexity.[2]

While these defence policy questions are not unique to Israel, the high frequency, magnitude and impact of security challenges facing Israel—as a small state—have been persistent. Historically, Israel has broadly distinguished two types of security threats: "basic or fundamental security" (*bitachon yisodi*) and "current security" (*bitachon shotef* or in short *batash*). The former refers to major conventional wars—real and potential that stipulated major risks for Israel's existence; the latter represented low-intensity conflicts, terrorist threats and attacks, border skirmishes, and enemy intrusions that harmed but did not seriously threaten the existence of Israel. The prioritisation of basic security, which has historically transcended all differences in ideology and politics, can be seen as the core of Israel's basic security concept based on deterrence, early warning and rapid military decision.

In this context, Israel has also traditionally distinguished three types of military commitments—so-called "circles of defence": (i) perimeter; (ii) intra-frontier; and (iii) remote commitments. Perimeter defence denotes conventional military threats to Israel's territorial integrity vis-à-vis large standing Arab armies in the immediate vicinity of Israel's frontiers (i.e. Egypt, Syria, Jordan); intra-frontier commitments refer to defence within Israel's territory principally against terrorist attacks and low-intensity incursions; and remote military commitments stipulates contingencies and threats at a considerable distance from Israel such as Iraq and Iran. During the Cold War, the predominant focus was on the "perimeter circle" that defined the frontlines of superpower rivalry in the Middle East and stipulated major conventional threats relevant to Israel's basic security. Yet, with the changes in the world order and systemic balance of power brought by the end of the Cold War in the early 1990s, Israel's strategic outlook has been shifting to a mixture of

---

1 Levite, Ariel. 1989. *Offense and Defense in Israeli Military Doctrine.* Jerusalem: Westview Press for Jaffee Center for Strategic Studies; Inbar, Efraim. 1996. "Contours of Israeli New Strategic Thinking." *Political Science Quarterly* 111 (1): 41-64; Inbar, Efraim. 1998. "Israeli National Security 1973-96." *The Annals of the American Academy of Political and Social Science* (558): 62-81; Cohen, Eliot, Andrew Bacevich, and Michael Eisenstadt. 1998. *Knives, Tanks, and Missiles: Israel's Security Revolution*. Washington D.C.: Washington Institute for Near East Policy; Creveld, Martin. 1998. *The Sword and the Olive: A Critical History of the Israeli Defense Forces.* New York: Public Affairs; Heller, Mark. 2000. "Continuity and Change in Israeli Security Policy." *Adelphi Paper* (IISS Adelphi Paper) (335): 1-82; Bar-Joseph, Uri. 2000. "Towards a Paradigm Shift in Israel's National Security Conceptions." *Israel Affairs* 6 (3): 99-114; Bar-Joseph, Uri. 2004. "The Paradox of Israeli Power." *Survival* 46 (4): 137-156; Bar-Joseph, Uri. 2008. "Lessons not Learned: Israel in the post Yom Kippur War Era." *Israel Affairs* 14 (1): 70-83;

2 Mofaz, Shaul. 1999. "The IDF Toward the Year 2000." *INSS Strategic Assessment* 2(2):1-10.

intra-frontier and remote military commitments. In the process, Israel's qualitative superiority in conventional defence has been offset or reduced by the increasing asymmetric capabilities and non-linear threats of neighbouring states as well as non-state actors.

It is within the context of these developments that the conceptual adoption and adaptation of cyber-oriented security debates gradually permeated into Israel's broader strategic debates. In the early 1990s, during the IDF Chief of Staff Ehud Barak's tenure, select Israeli defence analysts began to acknowledge the notion of "cyber activity" under the rubric of "future battlefield" [*sdeh hakrav haatidi*].[3] They analysed the emerging trajectory of information technologies used in combat, while observing the potential and implications of a new generation of precision-guided munitions, cruise missiles, command and control systems, integrated intelligence, and electronic warfare.[4] At that time, cyber security in the military domain was conceptualised along the lines of "information warfare" as a sphere of decisive importance in which achieving superiority in relation to the rival was seen as the key to deciding military conflicts.

In the civilian domain, government legislation and policy at that time focused primarily on information security—protection of data and computerised systems. For example, the 1995 Computers Law provided a legal framework for coping with civilian cybercrime, and the 1998 Law Ensuring Security in Public Bodies stipulated requirements for the protection of data and computer systems in specified government and private entities supplying infrastructure services, such as airlines and shipping companies, telephone and cellular communications companies, electricity suppliers and water companies.[5] The Israel Security Agency (ISA, Hebrew: *Shabaq*) was tasked with providing oversight and support for security at the Israeli embassies and selected state-owned enterprises.[6] This initial focus on the protection of computerised information infrastructures and databases characterised the first stage of Israel's national engagement with cyber defence.

Over the past decade, however, Israel's cybersecurity-related issues and policies have shifted with the increasing realisation of two key assumptions: (i) the accelerating expansion of cyberspace has increased political, military and socio-economic dependencies on the cyber domain by an order-of-magnitude, and select adversaries could in theory disrupt, destroy or subvert key strategic targets (i.e. critical infrastructures) without confronting the defending armies, and without exposure and clear attribution; (ii) existing civil/military compartmentalised organisational structures, responsibilities, policies and regulations for protecting computerised systems are not adequate to enable a comprehensive defence vis-à-vis the continuously evolving challenges and threats in cyberspace. In this context, "cyber" debate within and outside the Israeli defence establishment has shifted to the emerging threats, challenges as well as opportunities of cyberspace as a new medium for civil-military strategic interactions.

In particular, as more critical information infrastructure systems—from finance, energy, to transport—require telecommunications, clouds and computers connected to the Internet or proprietary networks, there is a growing awareness in Israel that different types of adversaries may seek to influence strategic outcomes by accessing and altering both the systems themselves and the data that resides within. In other words, an increased dependence on cyberspace by individuals, companies and organisations amplifies the vulnerabilities and potential for harm—not only of information, but also harm to persons, property and functional continuity of the state. Moreover, the realities of Israel's security environment predicate evolving cyber conflicts occurring not only during wartime or crises, but on a persistent basis—confrontations in and out of cyber space, including cyber-attacks on computerised systems, physical

---

3 Ben Israel, Isaac. 2012. "Introductory Remarks of the Annual Cyber Security International Conference 2012." Tel Aviv University. See also: Adamsky, Dima. 2010. The Culture of Military Innovation: *The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel.* p.98.

4 Brom, Shlomo. 1999. "Operation Desert Fox: Results and Ramifications." *INSS Strategic Assessment* 2 (1): 13-18; Cohen, Stuart. 1995. "The Peace Process and its Impact on the Development of a Slimmer and Smarter Israel Defense Force." *Israel Affairs* 1 (4): 1-21.

5 Interview with Deborah Housen-Couriel, Tel Aviv, August 10, 2014.

6 Tabansky, Lior. 2013. "Cyberdefense Policy of Israel: Evolving Threats and Responses." *Chaire de Cyberdefense et Cybersecurite*, Article no. III.12. Available at: http://sectech.tau.ac.il/sites/default/files/publications/article_3_12_-_chaire_cyberdefense.pdf

systems, and processes controlling critical information infrastructure, information operations, and various forms of cyber espionage.[7] In October 2013, for example, IDF's Chief of Staff Benny Gantz described what he believes will characterise Israel's future wars: Along with the border battles, which will also have serious implications for the Israeli civilian rear, "a vast cybernetic war will rage that will affect not only the military but also the civilian systems." It will be an "almost transparent" war, as media on both sides will cover it intensively in real time.[8]

Cyber Innovation in the Israel Defence Forces

During the recent Israel Defense Forces (IDF) operation code-named "Protective Edge" in Gaza in 2014, Israel faced large-scale cyber-attacks on its civilian communications infrastructure, including distributed denial of service attacks (DDoS) and Domain Network System (DNS) attacks from both state and non-state actors, traced to Qatar and Iran—Hamas' main benefactors.[9] Cyber attackers also targeted the IDF's 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.

Israel's strategy in responding to such threats are not so much about select advanced cyber-defence systems & technologies, but developing unique interdisciplinary methodologies in a multidisciplinary national "cyber-ecosystem" that integrates national research laboratories, military intelligence units, C4I organisations, the National Cyber Bureau, and start-up firms and entrepreneurs. In doing so, Israel is developing "a national cyber defensive envelope"—a multi-layered cyber defence strategy leveraging automated computerised systems and highly-trained personnel that proactively combine intelligence, early warning, passive and active defence, and offensive capabilities across civil-military domains.

At the core of Israel's cyber capabilities and sustained innovation drive, whether in the civil, military or commercial sectors, is the selection, training, research and development, skills and service experience of "cyber defenders" in the IDF. Indeed, the IDF is often credited for the creation and sustained success of the Israeli high-tech industry —by creating not only the key mechanisms (i.e. high skill training and its spin-off effects), but serving as "the main node in the national innovation system that diffuses information, spurs collective learning, and creates standards for the entire industry."[10] The process begins with the IDF identifying and recruiting suitable candidates excelling in subjects that have relevance for cybersecurity at selected top high-schools. Based on a range of qualifying exams, these students are placed in several of the IDF's cybersecurity units, including Mamram (*Merkaz Mahshevim UMa'arahot Meida*)—the Centre of Computing and Information Systems, which is the IDF's central computing system unit, providing data processing services for all arms and the general staff of the IDF; and its related unit (ii) the School for Computer Professions (*Basmach)*. Following graduation, recruits go on to serve in various IDF Military Intelligence and Manpower Directorate units, while some graduates are often offered a position in Mamram. The Mamram itself is part of Lotem Information Technology Division of the IDF's C4I Directorate, one of the largest security organisations in Israel developing technologies to thwart cyber-attacks and bolster Israel's defences against cyber warfare.[11]

While specific details of IDF's cyber units and capabilities are difficult to ascertain from open sources, well-known units of the IDF that specialise

---

7 Even, Shmuel and David Siman-Tov. 2012. "Cyber Warfare: Concepts and Strategic Trends." *INSS Memorandum* (117):1-91.

8 Harel, Amos. 2013. "Israel's Next War." *Haaretz* (October 12).

9 Lappin, Yaakov. 2014. "Iran Attempted Large-Scale Cyber-Attack on Israel, Senior Security Source Says." *The Jerusalem Post* (August 18).

10 Breznitz, Dan. 2002. "The Military as a Public Space: The Role of the IDF in the Israeli Software Innovation System." Industrial Performance Center and Department of Political Science Massachusetts Institute of Technology, MIT Working Paper IPC-02-004. Available at: https://ipc.mit.edu/sites/default/files/documents/02-004.pdf

11 IDF. 2013. "Hackers Beware: The IDF's Digital Battleground." *IDF Blog*. Available at: http://www.idfblog.com/blog/2013/10/09/hackers-beware-idfs-digital-battleground/

in various aspects of cyber defence (and offense) are frequently profiled in the media for their high levels of operational sophistication and their cutting-edge training of personnel. Among the most publicised are Intelligence Corps Unit 8200 which deals with SIGINT and code decryption;[12] the Cyber Unit within 8200, established in 2009; the C4I Directorate, leading network centric warfare;[13] and its two sub-units - the Cyber Defence Division, responsible for preventing and detecting infiltrations into military networks,[14] and Military Systems for Command Control (Matzpen) providing the systems and networks used by combat, planning and support organisations throughout the IDF.[15] In 2013, the IDF consolidated all aspects of its cyber situational awareness, intelligence, and command activities into a new cyber HQ, which is linked with the civilian Tehila (the governmental internet infrastructure) system, the E-Government project, and the newly established National Cyber Bureau. In 2013, the Israeli Ministry of Defence also announced the establishment of a new cyber directorate at the Mafat (the MOD Directorate of Defence R&D), which is tasked to conduct cyber R&D activities for select branches of the Israeli defence establishment by directly plug-in into cyber R&D capabilities of Israel's commercial high-tech sector.[16] By the end of the decade, IDF's C4I Directorate and key intelligence and information technology units will relocate from the IDF headquarters in Tel Aviv (Kirya) to Israel's new national cyber hub in Beersheba.

Operational aspect of these IDF cyber units are clouded in secrecy. However, press reports have linked Israel (and the United States) with the development of the *Stuxnet* virus, which disabled nuclear centrifuges in Natanz in 2010.[17] An additional example of Israel's operational cyber capabilities is Operation "Orchard", an Israeli airstrike on a Syrian nuclear facility in the Deir ez-Zor region during the night of 6 September 2007.[18] In this operation, the IDF combined elements of classical air power with an innovative cyber-attack that paralysed Syria's air defences. Operation "Orchard" is a prime example of the type of capabilities that nations may leverage in the future in utilising cyberspace as a force multiplier:

- Detection of future threats through sophisticated, cyber-enabled intelligence gathering, including satellite monitoring;
- Real-time intervention in enemy weapons systems or defensive systems, such as the Syrian air defence system in this case; and
- Utilisation of traditional air, sea or ground power in conjunction with cyber capabilities.

The deterrent effect of such mixed "kinetic-cyber" operations is not yet well understood, but one report of "Operation Orchard" noted that it restored Israel's credibility as a deterrent against Syrian forces, and also served as an effective signal to Iran.[19] A more recent example of Israel's use of its defensive cyber capabilities is the capture of the Iranian arms ship Klos-C in the Red Sea in March 2014, in Operation "Full Disclosure." The successful naval interception was carried out 1,500 km from Israeli shores, and was enabled as a result of the "advanced cyber and communications capabilities."[20]

---

12 Ingersoll, Geoffrey. 2013. "The Best Tech School on Earth is Israeli Army Unit 8200." *Business Insider* (August 13).

13 Dombe, Ami Rojkes. 2014. "Inter-Arm Tactical Communication." *Israel Defense (*June 29).

14 Katz, Yaakov. 2012. "First IDF Cyber Defenders Graduate." *Jane's Defense Weekly* (April 20).

15 Opall-Rome, Barbara. 2014. "Big Data Fortifies Israeli Cyber Defenses." *Defense News* (December 10).

16 Heller, Or. 2013. "New Cyber Directorate in Mafat." *Israel Defense* (December 3).

17 Sanger, David. 2013. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power.* New York: Broadway Books; *The Economist.* 2010. "The Stuxnet Worm: A Cyber-Missile Aimed at Iran." *The Economist (*September 24); UPI. 2010. "Enter Unit 8200." UPI (May 11): Available at: http://www.upi.com/Top_News/Special/2011/05/11/Enter-Unit-8200-Israel-arms-for-cyberwar/UPI-93881305142086.

18 Hersh, Seymour. 2008. "Why Did Israel Bomb Syria?" *The New Yorker* (February 11).

19 Ibid.

20 Dombe, Ami Rojkes. 2014. "The IDF is Ready for the Cloud Challenge." *Israel Defense* (April 14).

The 2010 National Cyber Initiative and the Establishment of the National Cyber Bureau

The progressive complexity in the cross-domain interactions of cyber threats coupled with constraints imposed by existing cyber-defence organisational structures has shifted the debate in the Israeli cyber security policy community. In 2002, Israel passed the National Security Ministerial Committee Resolution 84/B regarding the responsibility for protecting civilian computerised systems in the State of Israel. The Resolution 84/B became de-facto the national civilian cyber-defence policy, providing the initial framework for national Critical Computer Systems (CSS) policy.[21] At that time, Israel defined 19 "critical" systems, in both public and private domains, and dictated a "shared responsibility" for protecting their computerised systems between its users and regulators. In practice, a "user"—an organisation—would be tasked with financing, protection, maintenance, upgrading, backup and recovery of its critical IT systems, while sharing the information with the "regulator"—i.e. existing chiefs of security at government ministries. An oversight body, under *Shabak*, was created in the form of "National Information Security Authority" (NISA; *Re'em*).[22]

After nearly a decade, however, the baseline perspective and framework of the Resolution 84/B—the responsibilities, authorities, and functions of the governmental division and "special bodies" responsible for protecting civilian critical computerised systems have reached significant political and legal constraints. In particular, civilian systems and networks that have not been defined as essential became highly vulnerable to cyber threats, while the organisational responsibilities for the protection of computerised systems were deemed compartmentalised and fragmented.[23] Against this background, in November 2010, Prime Minister Benjamin Netanyahu appointed the Chairman of the National Council for Research and Development Prof Gen. (ret.) Isacc Ben-Israel to review existing policies and formulate a national plan for dealing with the growing cyber threat—the National Cyber Initiative. Specifically, Netanyahu noted its stated goal of:

> …preserving Israel's international status as a centre for the development of data technologies, and to provide the country with powerful capabilities in cyberspace to the end of ensuring Israel's economic and national resilience as an open and democratic knowledge-based society.[24]

Prime Minister Netanyahu also emphasised the need to position Israel in the leading five nations in the cyber field by 2015, in accordance with a vision of an Israel that maintains its global position as a centre of information technological development with powerful cyberspace capabilities. The detailed report eventually produced in May 2011 by the work of 80 experts who were involved in the Initiative was unprecedented in its scope, process and outcome. Eight sub-committees consisting of senior decision-makers and representatives, including the MOD Directorate of Defence R&D, the Chief Scientist of the Ministry of Economics, the National Economic Council in the Prime Minister's Office, the Ministry of Finance, the Ministry of Science and Technology, the Unit 8200 and the Unit for Telecommunications and Information Technology in the IDF, the Counter-Terrorism Headquarters in the National Security Council, National Information Security Agency (NISA), the Atomic Energy Commission, and other experts from the military, academia and government ministries convened over six months for discussions to draft recommendations to the Prime Minister and the Cabinet. A task force condensed these recommendations into a draft Government Decision 3611 to establish the National Cyber Bureau (NCB), which was passed unanimously on 7 August 2011.[25] The multi-disciplinary nature of the Initiative, and especially the tripartite cooperation among senior military, academia and government personnel, set the tone for the second phase of national engagement with cyber defence policy. Moreover, the end result was an operational Bureau within the Prime Minister's Office, which began its work formally in early 2012.

---

21 Tabansky, Lior. 2013. "Cyberdefense Policy of Israel: Evolving Threats and Responses." *Chaire de Cyberdefense et Cybersecurite*, Article no. III.12. Available at: http://sectech.tau.ac.il/sites/default/files/publications/article_3_12_-_chaire_cyberdefense.pdf

22 Ibid.

23 Levi, Ram. 2011. "The Fifth Fighting Space." *Israel Defense* (December 16).

24 Naftali, A. and Yuval Goren-Hezkiya. 2012. *The National R&D Council, Report for 2010-11* (in Hebrew), p. 10.

25 Government Decision 3611. 2011. "Advancing National Capabilities in Cyberspace." (August 7). Available at: http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf.

Figure 1: Strategic Challenges of Cyberspace: Interviews with Israel's Cyber Experts

Foreign Affairs and Defence	Society & Economy	Private Sector
• Attribution problems; ability to bypass military defences; • Blurring boundaries between peace and wartime; • Convergence with other asymmetric threats; • Absence of rules & legal norms; • Challenges of developing operational knowledge and concepts of cyberspace in relation to other warfighting domains; • Preserving IDF's qualitative advantage and technological sophistication: deterrence & offensive capabilities; • Intelligence sharing among various organisations in the security establishment; • Developing fundamental layers of defence: intelligence, early warning, passive defence, active defence, offense; • Interagency cooperation;	• Absence of borders; • Regulating organisational responsibilities and legislations for dealing with the cyber field; • Amplitude intensity of cyber threats to civil services, and services to private homes; • Threats to "concealed" computers, incl. navigational devices or controllers in cars; • Wide-scale psychological aspects; degradation of morale by cyber means; • Raising public awareness and resilience; • Comprehensive national monitoring and situational awareness; • Long-term planning of systems' infrastructures;	• Interdependencies between civil, military, and commercial sectors; • Changing cyber realities with a potential of sustained attacks on bodies or companies that could harm the State's functionality; • Industrial espionage; • Sustaining innovation in cybersecurity R&D; development of new technologies and tools, trained personnel, and national cyber strategy; • Fostering cyber innovation amid increasing internal/ global competition; • Constant future planning; partnership with defence sector;

Source: Author's interviews at the Annual Cyber Security International Conference, Tel Aviv University, 2014.

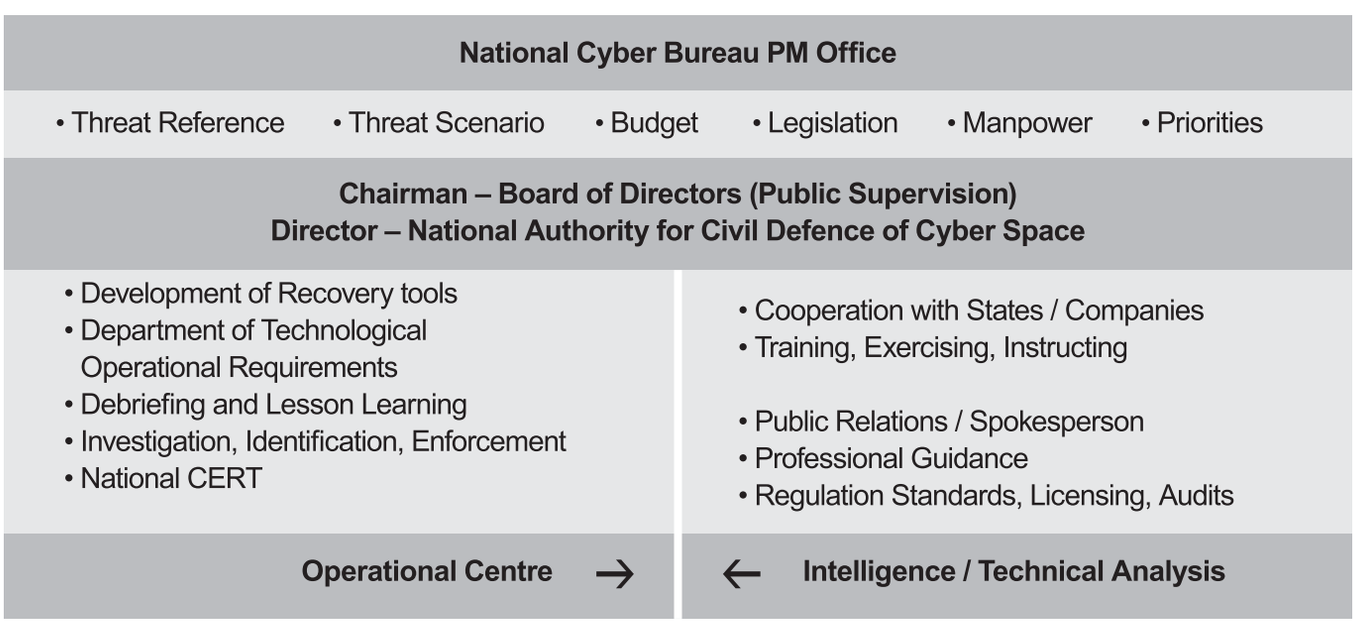
The NCB, reporting directly to the Prime Minister, brought a new interdisciplinary thrust in shaping the direction and character of Israel's civilian cyber security policy debates and capabilities. In particular, the NCB was tasked to advise the Prime Minister, the government and its committees regarding cyberspace (excluding military and foreign relations), to consolidate, guide, and inform about the governments' initiatives and efforts in devising national cyber policy, to provide national cyber-threat estimates by utilising relevant intelligence from all sources, to promote cyber R&D and industry, to increase public awareness on cybersecurity, and facilitate domestic and international cooperation on cyber-related issues. Essentially, these goals reflected key recommendations and findings of the National Cyber Initiative:[26]

[26] Tabansky, Lior. 2013. "Cyberdefense Policy of Israel: Evolving Threats and Responses." *Chaire de Cyberdefense et Cybersecurite*, Article no. III.12. Available at: http://sectech.tau.ac.il/sites/default/files/publications/article_3_12_-_chaire_cyberdefense.pdf

1. To promote the establishment of a national centre of knowledge and academic cyberspace R&D centres, particularly in the areas of high performance computing, code development, simulation and intelligence;
2. To develop a national cyber defence perimeter based on advances in domestic R&D and cybersecurity innovation;
3. To develop tools and operational capabilities for coping with cyberspace emergencies; whether in peacetime or wartime, while confronting moral, legal, and financial challenges;
4. To harmonise technical and non-technical legislative measures in line with international agreements such as the Council of Europe Convention on Cybercrime (2001)
5. Increase R&D collaboration between the military (IDF), defence industrial base, government, civilian industry, the academia, while mitigating the constraints of classification;
6. To improve export capacity for relevant cyber R&D solutions and technologies.

However, the NCB has been opposed and debated by the Shin Bet, internal security agency responsible for protecting critical civilian infrastructure for more than a decade, 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, tasked to coordinate and administer cyber policy and standards, is unable to carry out its mandate because it lacks intelligence-gathering capabilities, has no operational tradition of deterrence and no possibility of integration with similar security organisations worldwide.[27] On 21 September 2014, after nearly two years of policy turf battles, Prime Minister Netanyahu effectively rejected recommendations of the Shin Bet security services, and announced the establishment of a new government operational authority for cyber defence - the Operative Cyber Defence Authority (OCDA).[28] Notwithstanding the OCDA's mandate to bridge both security and civilian sectors in protecting Israel's national "space" from cyber attacks, organisational resistance to interagency cooperation coupled with unresolved issues of roles and missions remain as key policy challenges.

Figure 2: Framework for the Operative Cyber Defence Authority (OCDA) 2014



Source: Prof Isaac Ben-Israel; Presentation at the Vertex Innovation Forum 2014, Cyber Security & Financial Technology, Singapore, 2014.

---

27 Ravid, Barak. 2014. "Battle Move in Israel's Cyber Turf War: Shin Bet Loses Authority over Civilian Space." *Haaretz* (September 21).

28 Opall-Rome, Barbara. 2014. "Schedule Slips on Israeli Cyber Defense Command." *Defense News* (December 13).

Future Cyber R&D and the Role of the Private Sector

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 have been 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 per cent 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 per cent of global capital invested in the field of cyber security. According to the NCB, 14.5 per cent of all the firms worldwide attracting cyber-related investment are Israeli-owned.[29]

In this context, Israel is presently in the third stage of framing a national cyber defence vision. The missing element until now has been the private sector, which had only participated on the fringes of public defence policy discussions in the two earlier stages. The present national effort in the R&D and trade actively promotes the inclusion of this sector. Three of the leading stakeholders in Israel's national strategy to develop cutting-edge cyber and dual-use R&D: the MoD's R&D directorate (MAFAT), the Chief Scientist at the Ministry of the Economy, and the Ministry of Defence's Defence Export Controls Agency (DECA) are seeking policy initiatives that include the participation of the private sector. For example, the Office of the Chief Scientist provides assistance to start-up entrepreneurs through its network of 24 technological incubators around the country. More than 800 projects have been initiated, of which 600 have been completed. Another recent initiative within the Prime Minister's Office, called "Digital Israel", will further expand government-private sector collaboration as an integral part of the national vision.[30]

As part of a major national initiative to develop Israel's south, represented by the IDF's massive relocation to the region over the next few years, Israel is also developing the Beersheva Municipality as a leading cyber R&D hub. The Beersheva facility includes leading cyber industries such as EMC, Lockheed Martin, Deutsche Telekom, IBM and JVP; cutting-edge industrial academic research in the field of information security; leading government agencies such as the Cyber Bureau and the national CERT program; and next-generation educational frameworks.

Conclusion

Israel's evolving cyber defence strategy and debate must be linked to the changing strategic realities over the past decade—both internal and external, including the emergence of the varying cyber threat spectrum that has created yet another layer of asymmetric security predicaments, while mitigating the effectiveness of Israel's traditional deterrence, early warning and rapid military decision concepts. In the process, Israel has been developing a unique, symbiotic national "cyber eco-system" that integrates (i) leadership support for a national cyber defence vision; (ii) continuous upgrading of IDF's cyber defence/offense and intelligence capabilities such as in the Unit 8200; (iii) Israel's cutting-edge R&D programmes for boosting civilian and dual-use cyber capabilities embedded in the defence establishment, government agencies, private enterprise and the academia.

At the operational level, the IDF has focused on developing new operational concepts, methodologies and technologies for effectively shortening the cyber-version of a "sensor-to-shooter" cycle: intelligence (threat analysis & target creation), early warning and absorption readiness, cyber strike effort, active defence, command and control, passive detection, and ultimately, cyber deterrence. In the civilian arena, Israel's cyber strategy has been driven by the need for a pro-active, multi-disciplinary and inter-sectorial commitment. Its pace, direction and character is

---

29 Opall-Rome, Barbara. 2014. "Israel Claims $3B in Cyber Exports; 2nd Only to US." *Defense News* (June 20).

30 Ziv, A., Orpaz, I. and O. Hirshoga. 2013. "A New Bureau in the Prime Minister's Office Will Promote Israel's Digital Vision" (in Hebrew). *The Marker* (December 9).

dependent upon a much greater level of transparency and interagency cooperation among stakeholders, each one of which has a role to play in cyber defence.

While Israel continues to evolve the particular mechanisms of its cyber defence and cyber deterrence, it is appropriate to insert a word of caution about the Achilles heel of all innovative military and civilian cyber capabilities. The price of success of innovative systems is the perennial effort to continuously innovate. The various stakeholders in Israel's cyber eco-system must therefore fully commit and sustain this effort. Without a continuously updated, well-formulated national strategic policy and resource allocation for cyber security programmes, ensuring effective responses to cyber threats of the future may be at risk.

Figure 3: Policy Recommendations - Israel's National Cyber Initiative

Policy Objective:	**Advancing national cyber capabilities**
Key Goals:	• Organisation, integration and promotion of government-wide activities related to cyberspace, with a broad view that combines civilian and defence activities; • Develop a routine, state-wide operating procedures; preliminary preparedness for emergency cyberspace situations (including a national cyber situation room); • Promote cyber research and development through the relevant bodies, incl. the PBC and the Chief Scientist in the MOD Directorate of Defence R&D; • Promote cooperation between the private-business sector, the government sector, academia and the special bodies; • Examine Israeli legal systems with an eye on the developing cyber reality; advancing public awareness to issues related to cyberspace.
Recommendations:	• Establish academic research centres of excellence in the cyber field—strengthening scientific cyber research in Israel and establishing it as a world leader; • Establish infrastructure to develop cyber technologies such as developing simulation capabilities that resemble the cyber world or sections of it, and national authorisation for unclassified products and an estimation of their level of cyber protection; • Improve relevant export procedures in the cyber field; • Develop tools for cyber emergency situations—re-establishing and re-calibrating systems following attacks, ensuring continuity and restarting essential systems harmed in information events and attacks; • Develop a national cyber defensive perimeter—automatic computerised systems and human systems which, together, will provide defence for predefined computer systems; • Develop solutions for local defence—increasing the level of cyber security through a decentralised upgrading of various organisations' capabilities and among civilians; • Develop domestic cyber solutions and technologies—encouraging the development of Israeli products and information security solutions in order to reduce dependence on external bodies and to improve the technological capabilities of Israeli industry.

About the Author

Dr Michael Raska is a Research Fellow with the Military Transformations Programme at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University in Singapore. His research focuses on international security and defence issues, including theoretical and policy-oriented aspects of military innovation, force modernisation, and strategy.

About the Institute of Defence and Strategic Studies

The **Institute of Defence and Strategic Studies (IDSS)** is a key research component of the S. Rajaratnam School of International Studies (RSIS). It focuses on security research to serve national needs. IDSS' faculty and research staff conduct both academic and policy-oriented research on security-related issues and developments affecting Southeast Asia and the Asia Pacific. Its research agenda presently comprises the following programmes: Military Transformations, Military Studies, Maritime Security, Multilateralism and Regionalism, China, Indonesia, Malaysia, South Asia and the United States.

For more information about IDSS, please visit www.rsis.edu.sg/research/idss.

About the S. Rajaratnam School of International Studies

The **S. Rajaratnam School of International Studies (RSIS)** is a professional graduate school of international affairs at the Nanyang Technological University, Singapore. RSIS' mission is to develop a community of scholars and policy analysts at the forefront of security studies and international affairs. Its core functions are research, graduate education and networking. It produces cutting-edge research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-Traditional Security, International Political Economy, and Country and Region Studies. RSIS' activities are aimed at assisting policymakers to develop comprehensive approaches to strategic thinking on issues related to security and stability in the Asia Pacific.

For more information about RSIS, please visit www.rsis.edu.sg.

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

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