*Connections: The Quarterly Journal*
**ISSN 1812-1098, e-ISSN 1812-2973**

Lior Tabansky, *Connections QJ* 19, no. 1 (2020): 45-62
https://doi.org/10.11610/Connections.19.1.05

**Policy Article**

# Israel Defense Forces and National Cyber Defense

## *Lior Tabansky*

*Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv University*

**Abstract**: Cybersecurity in and of itself is not particularly new. Contemporary opportunities to exploit vulnerabilities, however, make this a challenging field. It is only natural that rivals exploit newly created opportunities. Conflict, in which adversarial relationships have a cyber dimension, is here to stay. Accordingly, societies must devise an appropriate organization to protect themselves from intentional threats. This article surveys Israel's approach, outlining the origins and the evolution of the national cyber defense, prevailing threats, doctrinal challenges, and the role military services play in cyber defense.

**Keywords**: Cybersecurity, cyber defence, strategy, doctrine, cyber operations, roles of the Israel Defense Forces.

Michael Warner, the Cyber Command Historian at the U.S. Department of Defense, outlined the main theoretical insights for American policy-makers and officials: Computers can spill sensitive data and must be guarded (1960s); Computers can be attacked and data stolen (1970s); We can build computer attacks into military arsenals (1980s and 1990s); Others might do that to us – and perhaps already are (1990s).[1] But new opportunities to exploit vulnerabilities make this a challenging field. It is only natural that rivals exploit such newly created opportunities. Cybered conflict, meaning that all adversarial relationships have cyber dimensions, is here to stay.[2] Accordingly, societies must devise and establish ap-

1 Michael Warner, "Cybersecurity: A Pre-History," *Intelligence and National Security* 27, no. 5 (2012): 781-799, https://doi.org/10.1080/02684527.2012.7085.

2 Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, GA/London: The University of Georgia Press, 2011).

propriate organizations to protect themselves from (intentional) threats. This article surveys Israel's national cyber defense origins, threats, and challenges.

## Israel's National Security Strategy and Current Strategic Environment

The core of Israel's security doctrine has always included:

- Absolute numerical inferiority[3]
- An acute lack of strategic depth[4]
- Constant regional volatility
- Protracted or irresolvable Arab-Israeli conflict
- Self-reliance in defense.

From the 1990s to 2010s, Israel's strategic landscape has shifted from threats originating in the Arab militaries to threats originating in irregular or semi-regular sub-state organizations supported by Iran. Iran, which is neither Arab nor a neighbor of Israel, poses a potential nuclear challenge of the highest magnitude and requires separate treatment. In contrast to states, organizations such as Hezbollah, Islamic Jihad, or Hamas build on a radical Islamist ideology denying Israel's right to exist. Their doctrine of resistance—*Muqawama*—assures its adherents that the long, historical, currently difficult struggle against Israel will eventually end in victory, despite temporary setbacks.[5] Hezbollah, Islamic Jihad, or Hamas organizations promise and claim success to their audiences, whereas Arab have states failed to defeat Israel. Yet Israel withdrew unilaterally from southern Lebanon in May 2000, disengaged from the main Palestinian popula-

[3] The combined population of the Arab states amounts to hundreds of millions, while Israel remains several orders of magnitude smaller. As of 2017, Israel was home to slightly more than 6.5 million Jews compared to some 400 million residents of the member countries of the Arab League – more than a third of them in countries bordering Israel.

[4] Yaakov Amidror, "The Evolution and Development of the IDF," in *Routledge Handbook on Israeli Security*, ed. Stuart A. Cohen and Aharon Klieman (Routledge, 2018), states: "From its very inception the State of Israel (and before it, the pre-state Jewish Yishuv) had to confront an existential security threat – a narrow territorial entity with its back to the Mediterranean Sea, surrounded on all sides by Arab foes sworn to its extinction. The distance from the Mediterranean Sea eastward to the mountainous area overlooking and dominating the coast—known as the "West Bank" and overwhelmingly populated by Palestinian Arabs—is merely 12 km at its narrowest (from Netanya to Tulkarm); and from Tel Aviv a mere 25 km (16 miles) at its widest. Even when adding the West Bank to the equation, the country's total width is less than 60 km. Israel's economic, financial, technological and demographic center is heavily concentrated along the Mediterranean seacoast on a narrow strip of just 100 km between Haifa and Ashdod."

[5] Efraim Inbar and Eitan Shamir, "'Mowing the Grass': Israel's Strategy for Protracted Intractable Conflict," *Journal of Strategic Studies* 37, no. 1 (2014), https://doi.org/10.1080/01402390.2013.830972.

tion centers in the West Bank after the Oslo accords and again in 2002, and evacuated its civil and military presence from the Gaza Strip in August 2005.

Israel's de-facto security strategy now includes four pillars:

I. Early warning

II. Decisive battlefield victory

III. Deterrence (cumulative, not absolute)

IV. Defense of the rear "home front."

The fourth—defense—has been added gradually after the lessons of the 1991 Iraq's ballistic missiles strikes, Palestinian terrorism, and the massive rocket threat from Lebanon and the Gaza strip. Supported by Iran, *Hezbollah* and *Hamas* deploy a massive firepower of more than 120,000 missiles and rockets aimed at Israel's cities. Iran drives modernization of their mostly short-range, low-precision arsenal to include precision-guided medium-range rockets. Israel's current operational arena has erased any meaningful distinction between military fronts and the civilian rear. The IDF increasingly invests in state-of-the-art military technologies to find ways to defend the "home front." The IDF cannot consider failure even at the tactical level, let alone think in terms of a protracted stalemate in future wars. Should deterrence or combat fail, neither Israelis nor the IDF will be given a second chance.

Unlike most Western militaries, cyber threats are not top of Israel's security agenda simply due to the high intensity of non-cyber threats ranging from terrorism to massive trajectory projectiles to missiles and Iran's nuclear program. Nevertheless, Israel has been one of the most advanced nations when it comes to the role of government in national cybersecurity. Non-military organizations performed the vast majority of cybersecurity.

The following sections present the civilian element first, and then the roles of the IDF.

## The Evolution of Israel's National Cyber Strategy

### *Critical Infrastructure Protection Arrangement of 2002*

Despite the prevalence of much more lethal and urgent non-cyber national security threats, Israel's government has been delivering Critical Infrastructure Protection (CIP) since 2003.

With a thorough understanding of civilian infrastructure and cyber vulnerabilities garnered from years of defense experience, at the turn of the century MAFAT (the Ministry of Defense R&D Directorate) communicated its concerns regarding the vulnerabilities of critical civilian infrastructure to other government branches. Eventually, the government then tasked the National Security Council (NSC) with outlining strategies to cope with the emerging risks. This resulted in the December 11, 2002 Government of Israel Special Resolution B/84 on "The responsibility for protecting computerized systems in the State of Israel." Israel created a CIP regulation that required supervised organizations to

appoint and employ dedicated IT-security personnel responsible for implementing the professional instructions of a government agency. The state decided to form a new CIP organization: *Re'em* (the National Information Security Agency, NISA). *Re'em* enjoyed the appropriate legal foundation in the 'Regulation of Security in Public Bodies Law of 1998' and the *Shabak* (Internal Security Agency) Statute. The supervised, privately-owned businesses and state-owned utilities maintain financial responsibility for all operations, protection, maintenance, upgrading, backup, and recovery of its critical IT systems—including the changes, enhancements, and equipment mandated by *Re'em*—all while sharing information and activities with the regulator. Finally, the law specified sanctions against executives of supervised organizations neglecting the mandatory requirements set by *Re'em*.

This Critical Infrastructure Protection arrangement has been in place since the B/84 Resolution of 2002. Since then, the government and defense sectors have fended for themselves, as Israel Police dealt only with strictly criminally defined cases of cybercrime. Therefore, as the first decade of the 21st century came to a close, this left the lion's share of the population—small-medium business (SMB), Non-Government Organizations (NGOs), and general citizenry—without cybersecurity. As the technology evolved, threat scenarios grew but received no treatment. These include potential disruption of civil services, accumulation of small-scale incidents in SMBs, risks to 'concealed' or embedded computers (such as navigational devices or controllers in cars), and degrading societal morale and resilience by cyber means (e.g., Influence operations via Social Media). Yet, only the experts dealt with the topic.

### *The National Cyber Initiative Expert Review*

The public discovery of Stuxnet in 2010 propelled cybersecurity to the top of policy agendas worldwide. Prime Minister Benjamin Netanyahu approached Major-General (Res.) Professor Isaac Ben-Israel, who at that time was the Chairperson of the National Council for Research and Development in the Ministry of Science, to review cybersecurity and recommend a policy for Israel. Professor Ben-Israel accepted the task, and the National Cyber Initiative was launched in 2010 with the vision:

> to preserve Israel's standing in the world as a center for information-technology development, to provide it with superpower capabilities in cyberspace, to ensure its financial and national resilience as a democratic, knowledge-based and open society.

The National Cyber Initiative addressed three main issues:

- How to incentivize and develop cyber technology in Israel to ensure its position as a (top five) world leader by 2015?
- Which infrastructures are required to develop cyber technology in Israel?

- What arrangements are required to best deal with the risks and threats in cyberspace?

The National Cyber Initiative thus clearly dealt with more than a narrow-defined national security. The composition of the task force reflected the initiative's broad vision and integrated approach. Consequently, for six months, 80 experts—defense and military representatives, academic experts, research and development institutional directors, and representatives from the relevant ministries—performed a systematic overview of the challenges and opportunities. The team was divided into eight subcommittees, one of which was classified.

### *Israel's National Cybersecurity Strategy of 2011*

The Government Resolution No. 3611 of August 7, 2011 "Advancing National Cyberspace Capabilities"[6] accepted the National Cyber Initiative's recommendations and it is Israel's public National Cybersecurity Strategy. Like all official high-level National Cybersecurity Strategy documents, it is a "grand strategy" that declares the vision and the guiding principles. Subsequent strategies in each domain have been derived from this grand strategy.

The main recommendation was to establish a dedicated government agency to lead cyber efforts across public and private Israeli stakeholders and to coordinate policy instruments. Further, the document recommended:

1. to establish a National Cyber Bureau (hereafter: The Bureau) in the Prime Minister's Office;
2. to regulate responsibility for dealing with the cyber field;
3. to advance defensive cyber capabilities in Israel and promote research and development in cyberspace and supercomputing;
4. to provide a budget for the implementation of the Resolution, proposed by the Prime Minister in consultation with the Minister of Finance and submitted to the government for approval within two months of passing this Resolution.

### *The Israel National Cyber Bureau (INCB)*

To develop and implement the grand-strategy, the Israel National Cyber Bureau (INCB) was established in the Prime Minister's Office (PMO).[7] Res. 3611 defined its mission and roles as follows.

---

6 Government decision 3611: Promoting national capacity in cyber space (Jerusalem, Israel, PMO Secretariat).

7 Dr. Eviatar Matania was named head of the INCB. He established the organization and directed its work. He served two three-year terms, remaining in duty until the end of 2018.

*Mission*:[8] The Bureau functions as an advising body for the Prime Minister, the government and its committees, which recommends national policy in the cyber field and promotes its implementation, in accordance with all law and Government Resolutions.

*Roles*:

- To advise the Prime Minister, the government and its committees regarding cyberspace. In matters of foreign affairs and security, the advice provided to the government, to its committees and to the ministers, will be provided on behalf of the Bureau by means of the National Security Council.
- To consolidate the government's administrative work and that of its committees related to cyberspace; to prepare them for their discussions and follow-on implementation of their decisions. In matters of foreign affairs and security, the consolidation of administrative work, preparation for discussions and follow-up on implementation of decisions will be carried out by on behalf of the Bureau by means of the National Security Council.
- To make recommendations to the Prime Minister and government regarding national cyber policy; to guide the relevant bodies regarding the policies decided upon by the government and/or the Prime Minister; to implement the policy and follow-up on the implementation.
- To inform all the relevant bodies, as needed, about the complementary cyberspace-related policy guidelines resulting from Government Resolutions and committee decisions.
- To determine and reaffirm, once a year, the national threat of reference in defending cyberspace.
- To promote research and development in cyberspace and supercomputing in the professional bodies.
- To work to facilitate the cyber industry in Israel.
- To formulate a national concept for dealing with emergency situations in cyberspace.
- To conduct national and international exercises to improve the State of Israel's preparedness in cyberspace.
- To assemble intelligence from all parties in the intelligence community regarding cyber security.

[8] The mission, roles, and tasks of the Israel National Cyber Bureau (INCB), presented in this section, are defined in "Advancing National Cyberspace Capabilities," Resolution No. 3611 of the Government, August 7, 2011, available at https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Israel_2011_Advancing National Cyberspace Capabilities.pdf.

- To assemble the national situation status regarding cyber security from all relevant parties.
- To advance and increase public awareness to threats in cyberspace and the means of coping with them.
- To formulate and publish warnings and information for the public regarding cyber threats, as well as practices for preventative behavior.
- To advance the formulation of national education plans and the wise use of cyberspace.
- To advance cooperation in the cyber field with parallel bodies abroad.
- To advance coordination and cooperation between governmental bodies, defense community, academia, industrial bodies, businesses and other bodies relevant to the cyber field.
- To advance legislation and regulation in the cyber field.
- To serve as a regulating body in fields related to cybersecurity, as detailed in Article I of Addendum B.
- To carry out any other role in the cyber field determined by the Prime Minister, in accordance with all laws and Government Resolutions.

*Tasks:*

The Head of the Bureau was tasked to submit to the Prime Minister, within 90 days of his appointment, a detailed work plan based on the working principles outlined by the Chairman of the National Council for Research and Development (NCRD), Prof. Maj.-Gen. (Ret.) Isaac Ben Israel, including:

- to approach the Council for Higher Education (CHE) and the Planning & Budgeting Committee (PBC) and request that they examine the possibility of establishing an academic cyberspace research center;
- to promote the establishment of a national center of knowledge for high-performance computing. If the center is academic, the *Malag* and *Vatat* [9] should be approached and asked to examine the matter;
- to establish infrastructure to develop cyber technology, such as developing simulation capabilities and national accreditation of cyber technology;
- to improve export procedures relevant to cyberspace and proper oversight of exports in this field;
- to develop tools for coping with cyberspace emergencies;
- to develop a national cyber defense;
- to develop solutions for defined cyber defense challenges;
- to develop domestic cyber solutions and technologies.

[9] See dedicated sections below.

### *Balancing Basic Liberties and Security Needs*

In June 2013, Edward Snowden began leaking secret documents he had stolen, revealing numerous global surveillance programs, many run by the United States' NSA, Australia's ASD, the United Kingdom's GCHQ, and Canada's CSEC often with the cooperation of telecommunication companies. These intelligence agencies collected bulk information and Snowden, among others, argued that these programs were degrading citizen's rights, especially to privacy, and were also violating domestic laws. Apparently, NSA taps directly into the servers of major internet firms, including Facebook, Google, Microsoft, and Yahoo, to track online communication using a surveillance program known as Prism.

At the time, the young INCB was focusing on force buildup, while the mature *Re'em* focused on CIP operations. As *Re'em* had been a unit of the *Shabak*, a potential risk loomed in the background. *Shabak* has a clear primary mission. A security or counter-intelligence organization that has access to other people's networks for a separate mission might take advantage of this access to a certain extent. It is true that *Shabak* had never abused the CIP assets for their purposes. It is also true that *Re'em* has had a good track record of success and that civilian oversight over *Shabak* had been well developed by 2010s. Nevertheless, the Snowden-NSA revelations propelled the liberties-security tensions to the top of the public debate as well as policy agendas. Any subsequent milestones in Israel's strategy must be set against this backdrop.

#### *The National Cyber Security Authority (NCSA)*

The Israeli government Resolution 2444 of February 15, 2015 established the National Cyber Security Authority (NCSA) to protect Israeli civilian cyberspace.[10] The NCSA was set up alongside the INCB in the PMO. Unlike CIP or cybersecurity agencies elsewhere, the NCSA has not been given any law-enforcement activities. This is a deliberate attempt to prevent any ongoing suspicion of NSA-like practices, to build trust, and to facilitate cooperation with all relevant cybersecurity stakeholders in the society. This unique design is intended to reduce the tension between basic freedoms and security, and to increase societal trust in this government authority. Following the same logic, the resolution is that NCSA incorporates the CIP organization *Re'em*. Indeed, it was transferred from the ISA (*Shabak*) to the NCSA in a process that took about a year.

The Authority began operations in the PMO on April 1, 2016, 90 days after Mr. Buki Carmeli was appointed head of the Authority. During the annual CyberWeek held by the Blavatnik Interdisciplinary Cyber Research Center (ICRC) of Tel Aviv University in June 2017, the NCSA held a one-day unveiling event, introducing its leadership and plans to a 600-strong audience. All the leaders of the NCSA presented their views and ideas. The head of the NCSA, Buki Carmeli, used the following water supply analogy to describe his vision of the NCSA:

[10] This decision was made after several rounds of extensive consultations, accepting Prof. Ben Israel's official recommendations.

> We (NCSA) approach civilian cybersecurity as public water system. We are concerned with uninterrupted supply of clean water throughout the society. When we will find contamination, we will not suspect who contaminated it, by negligence or malicious intent.

In 2017, all the cyber Bureau's technological activities were integrated into the Cyber Technologies Unit, which is the national technology arm for advancing cyber capabilities and technologies on a national level.

*The Computer Emergency Response Team – Israel (CERT-IL)*

Centered on cooperation, the NCSA has been developing a concept and the technology to enhance national situational awareness and security in cyberspace. The NCSA has established and operates the new National Computer Emergency Response Team (CERT-IL) to become a central public contact point for support for all civilian non-critical sectors. It is the central pillar in the long-term effort to secure Israel's civilian sector at large. While developing channels to work with sensitive data and clandestine agencies, CERT-IL must remain accessible to any civilian.

CERT-IL was planned and built in the Be'er-Sheba CyberSpark complex and began operations on July 1, 2014. An industrial consortium led by the Israeli defense contractor RAFAEL won the tender and built the CERT-IL.

*The Israel National Cyber Directorate (INCD)*

In accordance with Resolution 2444 of 2015, the NCSA, the operative body for cyber protection, and the INCB, responsible for the policies and the cyber force buildup, jointly constituted the National Cyber Directorate operating from the Prime Minister's Office, directly under the Prime Minister. The head of the Cyber Bureau was also appointed head of the Directorate and was put in charge of approving the work plans of the Authority and the budget of the Bureau. With the establishment of the NCSA, the guiding principle to insulate force buildup from daily needs led to a separate organization. Within two years, despite a good track record, the disposition changed towards a unified structure with a simpler hierarchy. To streamline the work, the Government of Israel Resolution 3270 of December 17, 2017 merged the Bureau and the Authority into the National Cyber Directorate, to be responsible for all aspects of cyber defense in the civilian sphere, from formulating policy and building technological power to operational cyber defense.[11]

[11] During this time, as Dr. Matanya completed his six-year term as Head of the Directorate, Mr. Yigal Unna was named his successor and took office at the beginning of 2018. Dr. Matanya then joined Tel Aviv University as Professor and Head of the Security Studies Program. See https://www.gov.il/he/Departments/policies/dec_3270_2017.

### *Strong Engagement of The Private Sector, NGOs and Academia*

The strategy is entirely cooperative, and in fact, the INCD has initiated, financed, and coordinated multiple efforts throughout Israel's economy. One example is the establishment and co-financing of Cyber Research Centers in most of the research universities in Israel. These academic centers of excellence perform independent scientific research. Another example is the establishment and co-financing of several innovation incentive programs in partnership with the Israel Innovation Authority. As for cybersecurity promotion throughout society, the INCD does not intend to introduce any additional regulations and, instead, has opted for cooperative work with existing regulators.

## IDF: Roles and Responsibilities in National Cyber Defense

The MoD and the IDF do not assume that their mission is to defend the entire society. The defense sector defends itself in cyber, whilst the INCD caters for all the rest. Such a division is common to all Western democracies.

As cybersecurity has become a profound risk, what does the IDF do about it? Major-General (Res.) Amidror writes:

> The IDF, like other militaries, is pre-occupied with working out how best to integrate cyber capabilities, for both defensive and offensive purposes. Since it is clear that cyber warfare will become hugely important in the coming years, and because there is a long road ahead, the IDF is already investing considerable sums of money and highly talented personnel in this area and is engaged in the deep and broad development of its cyber capabilities. How to organize the new units responsible for cyber, the relationship between offensive and defensive efforts, and the ratio between them – remain huge challenges.[12]

Current public sources suggest the following organization of Computer network operations (CNO) in the IDF.

### *Alleged Operations*

On September 6, 2007, the IAF successfully bombed and destroyed a building complex in Al-Kibar, near the city of Deir ez-Zor in eastern Syria. The building hid the construction of a graphite-cooled nuclear reactor: almost an exact copy of the plutonium reactor in North Korea.[13] The attack on the Syrian reactor project echoes the daring 1981 IAF raid, which destroyed the *Osirak* nuclear reactor in Iraq. But this time, a cyberattack was, allegedly, central to operational success: overcoming the dense Syrian air defense. According to foreign sources, the extensive Syrian air defense systems failed to identify the eight IAF fighter aircraft in the monitored airspace. These sources assume that Israel infiltrated and tem-

---

12 Amidror, "The Evolution and Development of the IDF."

13 Elliott Abrams, *Tested by Zion: The Bush Administration and the Israeli-Palestinian Conflict* (Cambridge University Press, 2013).

porary neutralized the Syrian air defense radars and communication systems in a cyber-attack. This 12-year old operation demonstrates the blurred line between electronic warfare and the cyber-warfare capabilities. Either way, it appears that a cyber-attack can play a supporting role for a kinetic strike.

The public disclosure of the Stuxnet malware in July 2010 and its subsequent analyses were an eye-opener for the public. Crucially, Stuxnet proved that a cyber-attack could indeed cause significant physical destruction. As Demchak and Dombrowski write:

> The Stuxnet method and its success thus changed the notion of vulnerability across increasingly connected societies and critical infrastructures. The days of cyber spying through software backdoors or betrayals by trusted insiders, vandalism, or even theft had suddenly evolved into the demonstrated ability to deliver a potentially killing blow without being anywhere near the target.[14]

The malware slowly damaged the centrifuges at the Natanz nuclear enrichment facilities in Iran by reprogramming the Siemens programmable logic controller (PLC) that ran the centrifuges and caused it to spin the motors out of the safe range. The stealthy, persistent attack within a secured air-gapped network had to first compromise a Microsoft Windows system and then propagate inside corporate networks to reach the programmable logic controller (PLC). By the end of 2010, Stuxnet had infected approximately 100,000 hosts in dozens of countries, 60 percent of which were in Iran.[15] Uniquely, Stuxnet infection does not equal damage. Stuxnet executed its weaponized payload (the PLC code supposedly altering the centrifuge rotation speed) only where the specific hardware and software configuration was found. No damage was done to an infected system that did not meet the precise set of predefined attributes.[16] Stuxnet is thus a precision-guided weapon: a cyber-attack that causes physical destruction but only to a specific target.

### *C4I & Cyber Defense (AGAF HA-TIKSHUV VEHAHAGANA BISVIVAT RESHET)*

In June 2015, the IDF published the decision to unify cyber units of the General Staff's C4I (command, control, computers, communications, and intelligence) branch and Military Intelligence under a single command by 2017. The IDF then reversed this plan to integrate defensive and offensive capabilities.

In May 2017, the IDF General Staff renamed the C4I branch (that was established in 2003) to The C4I & Cyber Defense branch. A recently established IDF Cyber Defense Division was merged into the C4I branch. C4I is now responsible

---

[14] Chris C. Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 32-61.

[15] Kim Zetter, *Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014).

[16] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365-404, https://doi.org/10.1080/09636412.2013.816122.

for network security within the IDF and remains responsible for IDF's Computer Network Defense (CND) and relevant Computer Network Exploitation (CNE). Moreover, the C4I will remain a central player in Israel's cybersecurity as it includes:

- training of IDF's Information and Communication technology professions;
- software development for the IDF;
- ICT system architecture for the IDF;
- cryptographic foundations development for the IDF and Israel at large.

The C4I & Cyber Defense branch aims to advance the vision of a single IDF network. However, insufficient cooperation, friction, and conflicts of interest between air and ground forces remain an unsolved problem in the IDF. Nevertheless, while ICTs have contributed to closer consultation, communication, and coordination during the last few years, this does not automatically create jointness.

This is not to accuse the IDF of a lack of jointness. In the business sector, one finds no less glaring siloes and uncoordinated activities as in any advanced military. With the increasing adoption of tailored cyber technologies within military siloes, the digital gaps between "elite" and common units are mounting. If left unattended, these developments may further impede jointness as well as prevent the coordination of cyber warfare throughout the IDF and other defense organizations in Israel.

This vision, of course, faces significant challenges: many of IDF's units and branches have developed and are operating diverse Information and Communication Technologies solutions on dissimilar infrastructures. A more likely outcome for the vision would be the unification of digital infrastructure within the IDF Ground Forces: C4I's natural domain.

### *Military Intelligence (Agaf haModi'in – Aman)*

Intelligence organizations have been the pioneers of cyber technology, amassing operational experience while remaining a step ahead of civilian capabilities. Israel's strategy puts a premium on both early warning and qualitative edge. These two factors are among the reasons why Israel's intelligence organizations have earned a formidable cyber reputation.

*Aman* is an independent service that is not part of the ground forces, the Navy, or the Air Force. *Aman* Unit 8200 is responsible for collecting signal intelligence (SIGINT) and for code decryption. According to intelligence analysts, 8200 is similar to the NSA or Britain's Government Communications Headquarters (GCHQ), often covering the entire intelligence cycle. Foreign sources assert that Unit 8200 contributed to Stuxnet, Flame, Duqu, and other sophisticated cyber campaigns for offense and intelligence.

Even so, Military Intelligence remains responsible for both Computer Network Attack (CNA) and relevant Computer Network Exploitation (CNE).

### The Israeli Air Force (IAF)

The Israeli Air forces view combat as the application of advanced high technology in waging war. The airplane embodies the supremacy of the advanced technology.[17] The IAF service culture is based on central command and control and supporting communications[18] and it aims to have a complete picture of the entire airspace in real-time. Headquarters accurately plan each air mission; time schedules are precise, determined by distance, flight path, evasion maneuvers, payload weight, and the amount of fuel. The IAF has developed and controlled its own supporting functions: Logistics; Command, Control, Communications, Computer (C4); Intelligence; Electronic Warfare (EW) and Special Force (the *Shaldag* unit) – all critical for air dominance. Practically, everything in the IAF depends heavily on advanced digital Information and Communication Technology. The IAF operates its own intelligence (*Lahak Modi'in – Lamdan*). As the IAF entirely depends on digital ICTs, the need to secure them was a consideration in design and operation, contributing to enhanced cyber maturity in the IAF. Moreover, the IAF has a separate and more advanced infrastructure than the other IDF branches.

### Spillover Effects of Defense R&D

In the mid-90s, Israel was a welfare state with a struggling economy and a negligible hi-tech industry. Just a few years later, while still coping with demanding security issues, Israel has developed into a technological giant with a sophisticated and innovative hi-tech sector. Today, the representation of Israeli hi-tech companies in the National Association of Securities Dealers Automatic Quotation System (NASDAQ) outstrips economic and technological superpowers such as Britain, Germany, Japan, and South Korea, and, for over a decade now, Israel has been one of the leading innovation hotbeds in the world. The IDF has created two spillover effects, which have contributed to Israel's success in high-tech and cybersecurity.

Given its overwhelming geographical and numerical inferiority, Israel's security strategy has been emphasizing a qualitative advantage that includes human skills, moral and scientific-technological superiority. The IDF perceives cyber technology as an important, broad, qualitative force multiplier. As in the US, several IDF branches and non-military intelligence organizations have long paid close attention to the development and exploitation of electronic warfare, signal intelligence, encryption and information security, computer warfare and information warfare. Almost three decades ago, several stakeholders within the IDF had already invested significant efforts in radical innovations that today would be termed "cyber warfare." Like DARPA in the US, *Maf'at* (the Ministry of De-

[17] Allen W. Batteau, "The Anthropology of Aviation and Flight Safety," *Human Organization* 60, no. 3 (Fall 2001), pp. 201-211.

[18] Amidror, "The Evolution and Development of the IDF."

fense Directorate for Defense Research & Development, DDR&D) has been driving and facilitating daring innovations in cyber R&D.

Regardless of what the IDF arms request, *Maf'at* can initiate major defense R&D independently. In parallel, the IDF's main cyber stakeholders—Intelligence, C4I, Air and Special Forces—have the capacity to perform tailored R&D and acquisition to support their missions.

In addition to classified R&D, *Maf'at* and the INCB launched a dual-use, civilian and defense cyber R&D plan called *MASAD* in October 2012.

### *Spillover Effect of Military Human Capital*

Swed and Butler postulate that the military socialization process cultivates new skills (human capital), new social networks (social capital), and new social norms and codes of behavior (cultural capital). Those three together are "military capital." Conscripts absorb the military capital, or part of it, while in service and "export" it into the civilian sphere where it converts well, especially in the hi-tech sector. For instance, improvisation, which is valued as a problem-solving skill in a resource-poor and uncertain environment and is, therefore, encouraged by the IDF culture while not being part of the official IDF code.[19]

Israel maintains mandatory conscription of 18-year olds. The IDF regularly trains and develops fresh recruits as well as career officers. Given the three-year mandatory service for males, one can assume that up to one-third of the force will be engaged in various training programs at any given moment. The IDF has long developed an intricate system to assess the conscripts' potential and assign a fitting training and career path to most, significantly contributing to the share of science and technology experts in Israel.[20] After the mandatory service, those who received valuable training are more likely to do reserve service than others are.

The profiles of Israeli hi-tech workers contain some very high military capital. Moreover, the job market in hi-tech demonstrates an institutional preference for those with military capital. Indeed, general and military service in technological units is perceived as such an advantage that it often equates to a University degree.[21]

---

19 Probably the most organized and influential group is the 8200 association. The name 8200 become hallmark since its graduates were the local hi-tech and venture capital industry vanguards. In comparison to other military veterans, Unit 8200 graduates' military capital convertibility is among the highest. See Ori Swed and John Sibley Butler, "Military Capital in the Israeli Hi-Tech Industry," *Armed Forces & Society* 41, no. 1 (August 2015), https://doi.org/10.1177/0095327X13499562.

20 Gil Baram and Isaac Ben-Israel, "The Academic Reserve: Israel's Fast Track to High-Tech Success," *Israel Studies Review* 34, no. 2 (2019), http://dx.doi.org/10.2139/ssrn3269147.

21 Swed and Butler, "Military Capital in the Israeli Hi-Tech Industry."

## *Doctrinal Challenges for IDF*

Cyber warfare and autonomous systems have clearly become a high defense priority. Which roles will the IDF assign for cyber capabilities? Consider one subset of questions: Should cyber capabilities support kinetic capabilities, should they replace kinetic strikes where possible, or should they deliver effects that will render kinetic force unnecessary? How well will the IDF make use of these? Significant change is as difficult for the IDF as for any other large bureaucratic organization.

### *Transparency vs. Secrecy*

Much of the challenges of cybersecurity are substantial. IDF Military services (in Hebrew '*Zroa'*) undergo significant rearrangements. However, the IDF cannot shake the habit of obscuring much of its activity, not only from the public but also from competing branches and services. These well-known tendencies to conceal activities impede cooperative intellectual efforts in commercial as well as military organizations. The following overview was performed without access to official sources. However, critical assessment is difficult when one is devoid of a shared factual base.

In 2010, the US DoD's decision to lift the self-imposed taboo on speaking about cyber-offense probably helped the IDF to state in 2012 that it was considering offensive cyber-warfare. In August 2015, the Israel Defense Forces (IDF) published its first formal defense doctrine, authored by IDF Chief of General Staff Lt. Gen. Gadi Eizenkot. The publication of the unclassified version of the IDF Strategy document formulated within the framework of the "Gideon" multi-year plan was a significant progress in civil-military relations. While not a binding document, the IDF Strategy outlined the military's view of strategic and operational responses to the main threats facing Israel and asked the political echelon for clearer instructions. The IDF Strategy outlined the principle to operate the force in contexts that are common to all operational theaters against a semi-state enemy and in the IDF's various functional situations: Routine, Emergency, and War.

### *Conceptualisation of Cyberdefense as Mabam*

The 2002, 2006, 2008-09, 2012, and 2014 rounds of large-scale violence demonstrate IDF's missions in the twenty-first century. The IDF developed the "campaign between wars" concept (*Mabam – Maaracha bein Milhamot*) to describe the military operations short-of-war, which IDF initiates and performs to thwart emerging enemy threats. This became an official doctrinal term later and was included in the summer 2015 IDF Strategy document. These covert and overt operations range from remote or on-the-ground intelligence collection, to surgical Special Forces raids, to precision strikes and to brigade-level combined arms maneuvers. The use of force is not intended to attain political goals, but rather to debilitate the capabilities of the enemy to harm Israel. For example, the range of strikes against Iranian forces in Syria and elsewhere often targeted weaponry shipments, key persons, or installations.

The *Mabam* concept appears to serve cybersecurity well. Mature cyber defense no longer singularly aims to prevent a breach. Nowadays, two models—the cyber kill chain and defense-in-depth—guide effective cyber operations. *Mabam* is an almost-routine emergency, which does not lend itself to a single-blow battlefield victory. Mature cyber defense similarly perceives the reality as an ongoing, long-term, adversarial competition. Advanced cybersecurity experts never promise complete defense, let alone a decisive victory. The goal is to minimize the threat through defense in-depth, intelligence and pre-emptive actions. The *Mabam* concept also accepts the less-heroic operational routine rather than decisive victory that destroys the adversary.

Whether the IDF at large or any of the stakeholders (C4I or Intelligence) consider cybersecurity on such terms is highly unclear.

### *Conceptualisation of Cyberdefense as Air Dominance*

This overarching quality-over-quantity strategy has led the IDF to a long record of operational accomplishment against the Arab states that practised military aggression. As a result, Egypt and Jordan have signed peace treaties and Assad's Syria has not fired a shot at Israel since 1982. These and other factors have led to the strengthening of the Air and Intelligence branches within the IDF.

The Air Force enjoys complete dominance and can operate against any ground, air, or naval target in the broader Middle East. The IAF became both the long strategic arm as well as the main contractor of precision fire, replacing the Artillery. This air dominance, of course, depends largely on the advanced exploitation of ICTs—cyber technologies—in all phases: planning; logistics; intelligence collection, analysis, and dissemination; C2; EW; defense suppression.

What would be the operational, strategic, and political benefits to the IDF if it aimed to assure cyber dominance? Inevitably, this would lead to drastic change. Much of cybersecurity practice seeks to minimize risks to the existing ways of "doing business." If your theory of victory rests on dominant armored maneuver, then you would need cybersecurity only as much as it can support operating armor units. If your theory of victory rests on manipulating the adversary's political decision-making process and calculus by means of persistent influence operations inter alia via Social Media, then cybersecurity would have a qualitatively different role.

## The Way Forward

For modern developed nations in general and for Israel, in particular, the national military have proven to be the most successful defense organization that provides security vis-à-vis other states. But, can militaries secure our societies from foreign cyber threats? To assume so is far from certain. Israel's defense expenditure ranges between 5% to 6% of its GDP – roughly four times the average of Western democracies. How much of this contributes to national civilian cybersecurity? Israel's National Cybersecurity Strategy accepts the division of responsibility between defense and civilian sectors: The Resolution 3611 does not

apply to "Special Bodies:" the Israel Defense Forces, the Israeli Police, Israel Security Agency (*Shabak*), the Institute for Intelligence and Special Operations (*Mossad*) and the defense establishment (mainly the defense-industrial base). The Directorate for Security of the Defense Establishment (*Malmab*) in the Ministry of Defense will remain the government's regulator for the cybersecurity of the defense sector.

The MoD and the IDF do not undertake the mission to defend the entire society in cyber. The defense sector defends itself in cyber, while the new national civilian organization has been established to cater for all the rest. Such a division is common to all Western democracies. Western militaries in general and the IDF, in particular, play an almost negligible role in providing national cybersecurity for their societies. Western military leaders must first face this reality and form a position on the desired military role in national cybersecurity. The range of options to enhance national cybersecurity can be derived from two general strategies:

- Get the militaries to provide more cybersecurity. This requires re-balancing between security and basic liberties so that Armed Forces could act within domestic civilian cyberspace
- Provide more cybersecurity without the militaries. This requires slashing conventional defense forces to free up resources for cybersecurity and establishing new civilian organizations.

Defense thinkers and leaders must invest major efforts in devising effective national cybersecurity, which will require radical innovation within defense establishments and elsewhere. Israel has been innovating with cybersecurity policies since 2002. While Israel has achieved relative success in civilian cybersecurity, more innovation is to be expected.

## Disclaimer



## Acknowledgement

Journal *Connections: The Quarterly Journal*, Vol. 19, 2020 is supported by the United States government.

## About the Author

Dr. Lior Tabansky is Head of research development, The Blavatnik Interdisciplinary Cyber Research Center of Tel Aviv University. Lior Tabansky offers a unique cybersecurity grasp, combining academic research in International Security Studies, 15 years of IT-pro work and business experience in formulating cyber strategies. Mr. Tabansky's 2015 book *Cybersecurity in Israel*, co-authored with Professor Isaac Ben-Israel, is the first comprehensive "insider" account of decades of Israeli policy and operations. Moreover, the book develops an original analysis of the roles grand strategy and innovation play in cybersecurity. Lior's doctoral dissertation reveals why even the most developed nations remain so exposed to destructive cyberattacks on strategic homeland targets by foreign states.
*E-mail*: cyberacil@gmail.com.