Briefing Memo

The Cyber Defense Organizations Protecting Israel's Critical Infrastructure and Related Challenges

SHIMAZU Takaharu

Military Strategy Division, Policy Studies Department

Introduction

Israel was ranked as a Tier Two country on a three-tier scale in the International Institute for Strategic Studies (U.K.)'s "Cyber Capabilities and National Power: A Net Assessment" report published in June 2021. Standing below Tier One, which is comprised solely of the U.S., Tier Two includes the U.K., Canada, and Australia, all part of the Five Eyes alliance, as well as China, Russia, and France. The report lauds Israel for having created both a vibrant cyber eco-system as well as a relatively high level of preparedness and resilience in the private sector through close cooperation between government agencies, private companies, academic institutions as well as international partners, led by the Israel National Cyber Directorate (INCD).[1]

On the other hand, the Israeli agencies responsible for cyber defense went through a decidedly disorderly transition reflecting numerous conflicting viewpoints before the civilian cyber defense posture of today was put in place, including its Critical Infrastructure Protection (CIP) policy. It has also been noted that there remain challenges to be resolved in terms of Israel's cyber security policies, including both legal and privacy concerns.

In light of such circumstances, this memo will review the evolution of Israel's cyber defense agencies in chronological order so that we may discuss the issues surrounding Israel's cyber security policies.

1. Israel's Critical Cyber Infrastructure

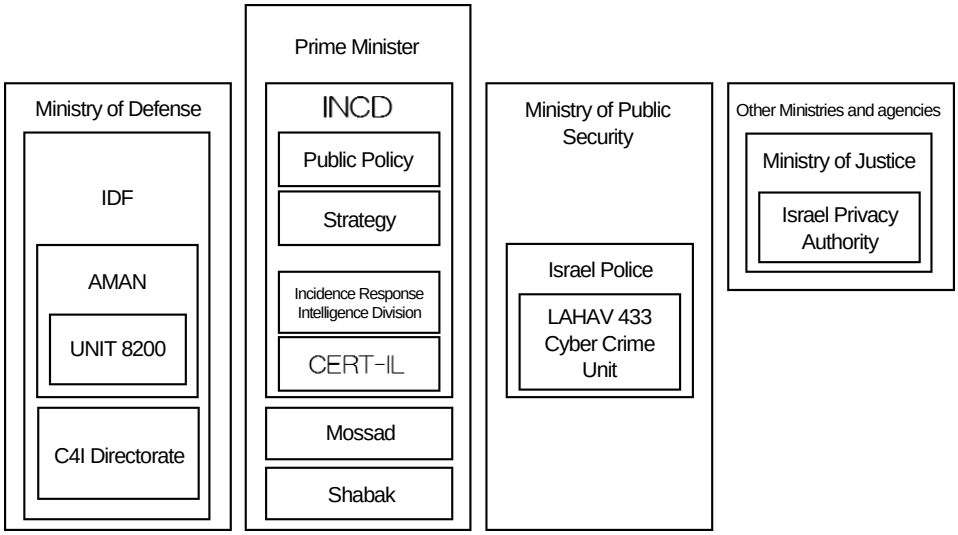
According to the INCD, critical cyber infrastructure is defined as the essential assets listed under the Law for Regulating Security in Public Bodies,[2] under which essential computer systems related to telecommunications, electricity, water, energy, finance, transportation, and other areas as well as the data and confidential information handled by these systems are subject to protection.[3] As such, public bodies and the essential computer systems they manage, both of which are regulated by the national government under the law, can generally be considered to be recognized as "critical infrastructure."

2. Israel's Cyber Defense Organizations

The figure below provides an overview of Israel's cyber defense organizations.

[1] "Cyber Capabilities and National Power: Net Assessment," IISS, June 28, 2021, p. 69, https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.
[2] Israel National Cyber Directorate, "Cyber glossary for professionals," INCD website, https://www.gov.il/he/departments/general/terms.
[3] "Law for Regulating Security in Public Bodies, 5758-1998," NEVO, https://www.nevo.co.il/law_html/law01/111m1_001.htm.

Overview of Israel's Cyber Defense Organizations



Source: Prepared by author based on Israel's "National Cybersecurity and Cyberdefense Posture Policy and Organizations," Center for Security Studies (CSS), ETH Zürich, p. 14.

Today, Israel's civilian cyber defense primarily falls under the responsibility of the INCD and Shabak (known as the Israeli Security Agency), Israel's internal security service.[4] Both agencies report directly to the Prime Minister, and a description of each is given below.

(1) The INCD

Under the direct command and supervision of the Prime Minister and his office alongside other organizations such as Shabak and Mossad, the INCD plays an important role in Israel's cyber defense.[5] The context behind how it came to be in its current position will be described in the next section, but its main mandate includes responsibility for all aspects of cyber defense in the civilian sphere, from formulating policy and building technological power to actual operational defense activities in cyberspace.[6]

It also manages the Israeli Cyber Emergency Response Team (CERT-IL), an operational unit that supports the INCD's activities and is responsible for maintaining a 24/7 reporting mechanism between the INCD, public bodies, and privatized public bodies throughout the entire State of Israel.[7]

The entities that fall under the INCD's jurisdiction are specified in supplementary provision 5 of the Law for Regulating Security in Public Bodies and include the Bank of Israel, Israel Natural Gas Lines, Energy

[4] Other cyber defense agencies include Israeli Defense Forces (IDF) Unit 8200 and the C4I Directorate under the Ministry of Defense, as well as the Israeli Police LAHAV 433 Cyber Crime Unit. Jasper Frei, "Cyberdefense Report: Israel's National Cybersecurity and Cyberdefense Posture Policy and Organizations," Center for Security Studies, ETH Zurich, September, 2020, p. 15, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf.
[5] Ibid., p. 7.
[6] IISS, "Cyber Capabilities and National Power," p. 73.
[7] Israel National Cyber Directorate, "The Israeli Cyber Emergency Response Team (CERT)," INCD website, June 5, 2019, https://www.gov.il/en/departments/news/119en.

Infrastructures (PEI), Israel National Water Co., Israel Electric Corporation, Israel Post, Ben Gurion Airport, Israel Railways, the Israel Broadcasting Authority, the Ministry of Finance, the Ministry of Transport and Road Safety, and the Civil Aviation Authority.[8]

(2) Shabak

Shabak is Israel's internal security service tasked with counterterrorism operations. Alongside the INCD, it is responsible for cyber defense and reports directly to the Prime Minister.[9]

Shabak's involvement in cyber defense relates to its responsibility over essential telecommunications infrastructure. Under supplementary provision 4 of the Law for Regulating Security in Public Bodies, the organizations regulated by Shabak include the major Israeli telecommunications operators Bezeq (which operates landlines, mobile communications, ISPs, etc.), MedNautilus Israel (which operates submarine cables), Pelephone Communications (which operates mobile phone services), and Hot Telecommunication Systems (which operates cable TV and broadband telecommunication services).[10]

3. The Evolution of Israel's Cyber Defense Organizations

(1) The National Information Security Authority's Heavy-Handed Operations and Increased Cyber Threats against Small- and Medium-sized Businesses

Dissatisfied with the measures taken by existing state organizations to deal with threats that had arisen alongside the emergence of the computer-based society, the Israeli Government ordered the National Security Council (NSC) to formulate a strategy to address such threats. On December 11, 2002, Special Resolution B/84 on "the responsibility for protecting computerized systems in the State of Israel" was passed,[11] which included a mandate that a government organization be created to protect civilian computer infrastructure. This resulted in the establishment of both a steering committee comprised of representatives from concerned bodies, as well as the National Information Security Authority ("Re'em" in Hebrew) installed within Shabak.[12]

At the time, Re'em was given authority to monitor IT security in organizations defined as "critical," issue directives, oversee their execution, and even impose sanctions on organizations that violated the directives Re'em had mandated.[13] It was also permitted to access any data or assets in relevant organizations' possession to ensure compliance with its directives and assess new risk factors.[14] The majority of the population, though, including small- and medium-sized businesses, NGOs, and the general public not deemed critical by Re'em were left without cyber security, going underserved in the face of technological advances and growing threats

[8] "Law for Regulating Security in Public Bodies, 5758-1998."
[9] Shabak (or Shin Bet) is an abbreviation of Shirut HaBitahon HaKlali (Hebrew for "General Security Service.") Shabak website, https://www.shabak.gov.il/english/pages/about.html#=1.
[10] "Law for Regulating Security in Public Bodies, 5758-1998."
[11] Lior Tabanski & Isaac Ben Israel, *Cybersecurity in Israel*, Springer, 2015, p. 35.
[12] Ibid.
[13] Ibid.
[14] Tabanski & Ben Israel, *Cybersecurity in Israel,* p. 38.

for the first decade of the 21st century.[15]

(2) The INCB's Establishment as Israel's First Civilian Cyber Defense Agency and Conflicts with Shabak

In 2010, then Israeli Prime Minister Benjamin Netanyahu ordered retired Major General Isaac Ben-Israel, Chairman of the Israel National Council for R&D, to review Israel's current cyber security policies. The National Cyber Initiative was then submitted that same year,[16] and in turn, Government Resolution No. 3611, "Advancing National Cyberspace Capabilities," was passed on August 7, 2011.[17]

The main component of Government Resolution 3611 was the establishment of a specialized government agency to take the lead on cyber activities involving public and private stakeholders in Israel and coordinate the policy-related aspects therein; namely, it created the Israel National Cyber Bureau (INCB).[18] The INCB was primarily tasked with recommending cyber sector policies to the Prime Minister, the government, and government committees, as well as with drafting a comprehensive national cyber strategy.[19] Yet due to unresolved disagreements with other concerned agencies, it failed to drive change in Israel's CIP efforts.[20]

(3) The Transfer of CIP Duties from Re'em and the Creation of the INCD as a Civilian Cyber Defense Agency

Prime Minister Netanyahu ordered retired Major General Isaac Ben-Israel, who had the 2010 National Cyber Initiative developed, to create a roadmap to resolve the impasse over cyber security policy.[21] The resulting recommendations that Ben-Israel submitted to Netanyahu became the basis for a change in policy,[22] and on February 15, 2015, Government Resolution 2443, "Promoting National Regulation and Government Leadership in Cyber Defense," was passed,[23] which called for the creation of a new agency to advance civilian sector cyber security.[24]

The new agency was called the National Cyber Security Authority (NCSA) and placed in charge of cyber defense operations under the Prime Minister's office alongside the INCB, which was responsible for developing and maintaining Israel's cyber defense capabilities.[25] On the same day, Government Resolution 2444, "Promoting National Preparedness for Cyber Defense,"[26] was passed, with the NCSA absorbing Shabak's

---

15 Ibid.; Lior Tabanski, "Critical Infrastructure Protection against Cyber Threats," Military and Strategic Affaires Volume 3, No. 2, INSS, November, 2011, pp. 72-73, https://www.inss.org.il/wp-content/uploads/2017/01/Military-Strategy-volume-3-no.2.pdf.

16 The initiative made a proposal for how to incentivize the development of cyber technologies, what infrastructure would be required for said development, and what arrangements would be needed to best address dangers and threats in cyberspace in order to solidify Israel's position as one of the top five countries in cyber by 2015. Tabanski & Ben Israel, *Cybersecurity in Israel*, p. 43.

17 Lior Tabanski, "Israel Defense Forces and National Cyber Defense," *Connections: The Quarterly Journal*, Volume 19, Issue 1, January 19 ,2019, p. 49, https://isij.eu/article/israel-defense-forces-and-national-cyber-defense.

18 Ibid.; Prime Minister's Office, "Government Resolution 3611: Promoting National Capacity in Cyberspace," Prime Minister's Office, July 8, 2011, https://www.gov.il/he/departments/policies/2011_des3611.

19 Tabanski & Ben Israel, *Cybersecurity in Israel*, p. 52.

20 Ibid., p. 57.

21 Ibid.

22 Ibid.

23 Prime Minister's Office, "Government Resolution 2443: Promoting National Regulation and Government Leadership in Cyber Defense," Prime Minister's Office, February 15, 2015, https://www.gov.il/he/Departments/policies/2015_des2443.

24 Tabanski & Ben Israel, *Cybersecurity in Israel*, p. 58.

25 Ibid.

26 Prime Minister's Office, "Government Resolution 2444: Promoting National Preparedness for Cyber Defense," Prime Minister's Office, February 15, 2015, https://www.gov.il/he/Departments/policies/2015_des2444.

subordinate division Re'em and assuming the CIP duties it had been carrying out up until that point.[27] In 2016, the following year, the transfer of jurisdiction over essential computer systems was complete. Responsibility for telecommunications operators remained with Shabak as per the aforementioned Law for Regulating Security in Public Bodies, while the NCSA was given jurisdiction over the other computer systems and organizations provided for in supplementary provision 5 of the law.[28]

The resolutions also established the CERT-IL within the NCSA as a central hub for cyber security incident management and response to strengthen national resilience against cyber threats,[29] and the aforementioned Government Resolution 2444 simultaneously approved the creation of the Israel National Cyber Directorate (INCD) as well.[30]

(4) The Formulation of the National Cyber Security Strategy and Establishment of a Civilian Cyber Defense Posture

Government Resolution 3270[31] of December 17, 2017 merged the INCB and NCSA into the INCD, making the Directorate responsible for all aspects of civilian cyber defense from formulating policies to building technological capacity and engaging in operational cyber defense.[32] On December 27, 2018, Israel's parliament, the Knesset, passed an amendment to the Law for Regulating Security in Public Bodies that provided a legal basis for merging the agencies into the INCD as mentioned above.[33]

The INCD's[34] role in the civilian sector, its operational concept, and its approach to capacity building were made clear when Israel published its first "National Cyber Security Strategy In Brief"[35] ("Cyber Strategy") in September 2017. In its current state, the INCD issues policies and guidance.[36]

4. Israel's Cyber Security Policy Challenges

(1) Lack of Legal Basis for the INCD's Own Operations

As seen thus far, Government Regulations B/84, 3611, 2443, 2444, and 3270 shaped Israel's civilian cyber security systems and posture, with the Cyber Strategy formulated in 2017 clarifying the relevant agencies'

---

27 Tabanski, "Israel Defense Forces," p. 52.
28 Israel National Cyber Directorate, "Government decisions and the law regulating security in public bodies," INCD website, July 16, 2018, https://www.gov.il/he/Departments/news/govdecisions.
29 Tabanski & Ben Israel, *Cybersecurity in Israel*, p. 58.
30 Tabanski, "Israel Defense Forces," p. 53.
31 "Government Resolution 3270: 1. Consolidation of units of the national cyber system 2. Granting an exemption from a tender for the position of head of the national cyber system 3. Addition of the position of head of the national cyber system to the addendum under section 23 of the Civil Service Law (Appointments) 4. Determination of salary and terms of service," Prime Minister's Office, December 17, 2017, https://www.gov.il/he/departments/policies/dec_3270_2017.
32 Tabanski, "Israel Defense Forces," p. 53.
33 Global Legal Monitor, "Israel: Knesset Passes Amendment Law Recognizing Role of National Cyber Directorate in Protecting Cyberspace," Library of Congress, July 22, 2019, https://www.loc.gov/item/global-legal-monitor/2019-07-22/israel-knesset-passes-amendment-law-recognizing-role-of-national-cyber-directorate-in-protecting-cyberspace/.
34 The INCD's role in civilian cyber defense falls under the NCSA in the Cyber Strategy report as the agency had not yet been merged into the INCD at the time of publication.
35 Israel National Cyber Directorate, "Israel National Cyber Security Strategy In Brief," Prime Minister's Office, September, 2017, https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf.
36 Israel National Cyber Directorate, "Israel National Cyber Directorate," https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page.

operational concepts. Over the years, the INCD has issued policies and recommendations, played its role leading the private sector, and at the same time running the CERT-IL to respond to incidents on a day-to-day basis.

However, the tentatively named Cyber Protection Law that would provide a legal basis for the INCD to fulfil its obligations as an operational agency for civilian cyber security has yet to be put in place (as of December 17, 2021), leaving the INCD's duties, functions, and powers legally undefined.[37] It is also said to not possess the same legal force or investigative authority as law enforcement agencies in carrying out cyber security operations.[38] Before the bill was submitted in 2018, then Director General of the INCD Yigal Unna said that the law "formalizes what we do today" and establishes a framework for what Israel's civilian and government sphere should be doing in the field of cyber security.[39] This statement suggests that the INCD is providing recommendations and formulating policy without any legal basis.

(2) Moves to Pass the Cyber Protection Law (Tentative) to Strengthen the INCD's Authority and Concerns Therein

Legislation on cyber defense has been in the works since 2018, citing the need for it in response to the growing threat of real-world cyber-attacks,[40] but has failed to pass in the face of strong domestic opposition.[41] The main objections to the 2018 bill were reportedly (1) the broadly defined authority given to the INCD (including the power to enter private property and seize evidence without a court order), (2) insufficient privacy protections, (3) the weak mechanisms for monitoring the INCD's activities, and (4) conflicting authority with Shabak and other law enforcement agencies, intelligence agencies, and the military.[42]

In light of the pandemic-induced spread of remote work, heightened cyber security risks as digitalization progresses, and repeated cyber-attacks against Israeli companies, Prime Minister Netanyahu announced a new bill entitled "Cybersecurity and the National Cyber Directorate" in February 2021 to promptly address these challenges.[43] The new bill was seen as an abbreviated version of the 2018 bill and was framed as temporary legislation.[44]

The new bill aims to legally establish the INCD's functions and powers in providing expert cybersecurity guidance to government agencies, other public bodies, and private entities, but as with the 2018 bill, serious doubts were raised about the intrusive powers it would grant the INCD with no exceptions in undertaking cyber

---

[37] Global Legal Monitor, "Israel: Knesset Passes Amendment Law."
[38] Tabanski, "Israel Defense Forces," p. 52. The NCSA was not granted the authority to engage in law enforcement activities when it was established in 2015, believed to be the result of careful deliberation in the aftermath of Edward Snowden exposing the actions of the U.S. NSA and other agencies in 2013.
[39] Shoshanna Solomon, "Winter is still coming,' cyber chief warns on hacking threats," *Times of Israel*, June 20, 2018, https://www.timesofisrael.com/winter-is-still-coming-cyber-chief-warns-on-hacking-threats/.
[40] Global Legal Monitor, "Knesset Passes Amendment Law."
[41] Deborah Housen-Couriel, Tal Mimran, Yuval Shany, "Israel's Version of Moving Fast and Breaking Things: The New Cybersecurity Bill," LAWFARE, May 7, 2021, https://www.lawfareblog.com/israels-version-moving-fast-and-breaking-things-new-cybersecurity-bill.
[42] Amir Cahane, "The New Israeli Cyber Draft Bill – A Preliminary Overview," The Federmann Cyber Security Research Center, 2018, https://csrcl.huji.ac.il/new-israel-cyber-law-draft-bill; In fact, a leak to the media revealed that the military among others had opposed Prime Minister Netanyahu's plan to strengthen cyber security a year before the bill was released. Jacob Magid, "Security chiefs slam Netanyahu over planned cyber defense body," *Times of Israel*, April 24, 2017, https://www.timesofisrael.com/security-chiefs-slam-netanyahu-over-planned-cyber-defense-body/.
[43] Deborah Housen-Couriel, "Israel's Version of Moving Fast and Breaking Things."
[44] Ibid.

defense operations on private computer networks. The INCD could, for example, seek a court order allowing it to access a private company's servers without its consent should the company fail to cooperate. The bill would also allow the data collected to be shared among government agencies, raising concerns over data protection and leaks, privacy protections, and intellectual property rights.[45]

Conclusion

Israel is capable of leading the world in cyber security as one of the world's top high-tech nations in the field, which is surely what secured its place as a Tier Two country in the IISS' cyber capability report mentioned at the beginning of this memo.

At a time of increased risk of cyber-attack caused by heightened tensions between Israel and Iran, providing the INCD with new legal tools as soon as possible to protect Israel's national security interests in cyberspace has become all the more urgent.[46] However, when it comes to civilian cyber security, no common ground on the Cyber Protection Law (tentative) has been found and it has yet to be enacted.

There is a seemingly global trend toward greater state involvement in cyber defense, including the protection of critical infrastructure, but at the same time there is concern that state involvement in and excessive monitoring of the activities of individuals and private corporations in the name of maintaining public order and protecting national interests may discourage voluntary efforts by the private sector and undermine any incentives to develop new technologies. Thus, in operating cyber defense agencies like the INCD and Shabak, certain considerations need to be given to private individuals and companies and a system be established to ensure that the agencies carry out their operations properly.

[45] Ibid.
[46] Ibid.