BESA
The Begin-Sadat Center
for Strategic Studies
Bar-Ilan University
PERSPECTIVES
THE BEGIN-SADAT CENTER FOR STRATEGIC STUDIES

Analysis and Recommendations for Israel's New National Cyber Strategy

by Col. (res.) Shay Shabtai

BESA Center Perspectives Paper No. 2,349, July 17, 2025

EXECUTIVE SUMMARY: The Israel National Cyber Directorate (INCD) recently published an update of the country's cyber security strategy. While the new strategy develops and updates the principles of its 2017 predecessor, it differs in its fundamental concept. The new version derives from broad national objectives in the cyber domain and focuses on protecting the means of securing core national processes and infrastructure. It addresses issues such as how to define the whole of national cyber security and how to deal with the technological supply network. The document is also influenced by the Iron Swords War in several ways. The strengths of the INCD should be built to the point that it can position itself as a leading part of the governmental and national cooperation network that will be required for implementation.

What's in the new strategy?

In February 2025, the Israel National Cyber Directorate (INCD) published an update of the National Cyber Security Strategy. [*Disclosure: The author assisted in this endeavor by publishing* National Cyber Strategy: Issues for Discussion *at the BESA Center and by engaging in dialogue with the INCD.*] The document, which replaces its predecessor from 2017, is clear and intuitive. It defines the national vision of national cyber security this way: "A trustworthy, reliable and safe digital space that enables the benefits of a thriving and advanced world."

The document outlines four overarching principles for implementation that are to form the basis for response efforts:

1. **Joint security** - combined action by the government and other sectors (a "whole-of-society effort")
2. **Active security –** taking a proactive approach to security
3. **Leveraging innovation and technological excellence for better security** - building on the comparative advantage of Israel's national technological ecosystem in the cyber field
4. **Resilience and crisis management** - preparing for crises that will certainly occur

The document then breaks down the key response efforts and their sub-components according to three pillars:

1. ***Securing the national cyber space:*** This refers to efforts to protect state assets. The key efforts within this pillar are safer citizens and stronger businesses, more resilient critical and essential services, and spatial security.
2. ***The national formation:*** This involves the integrated organization of all state agencies. The main efforts here are joint security, readiness for cyber surprises and digital emergencies, and proactive threat elimination.
3. ***Developing strategic partnerships and future capabilities*****:** The main efforts of this pillar are the development of infrastructure for cooperation and partnerships and an investment in quality capacity-building to maintain Israel at the forefront of global cyber security.

Comparison with other documents

The basic concept of the new strategy is fundamentally different from that of the 2017 version. The earlier strategy positioned cyber as a component in a broad national context and defined the state's cyber vision this way: "The State of Israel will be a leading state in harnessing cyberspace for the benefit of its economic growth, social welfare, and national security". That version dealt with cyber - as the state had done ever since the National Cyber Initiative of 2011 - as a generator of national strength, with the issue of security a derivative thereof. Security is mentioned only in the document's aim: "To regulate all national efforts in the field of cyber security, to create a 'common language'

among those engaged in the profession, and to ensure a stable and long-term response".

The new strategy goes more deeply into the realm of cyber and focuses on securing the State of Israel. With that said, there is continuity in the two documents' concepts of action. In the previous strategy, the focus was on three layers: economic resilience, systemic resilience, and national security. The new strategy updates these layers in light of the progress achieved since 2017. The updates include, for example, a framework for implementation in the security apparatuses of government sectors and government computing infrastructures.

The change in approach in the basic concept is reflected in the new document's reference to technological innovation and international collaboration. The previous document identified both as supporting efforts for the strategy's implementation. The building of national scientific-technological capabilities involved the state's fostering of entrepreneurship and technological innovation in the Israeli cybersecurity industry and support for dedicated research centers at academic research institutions. The new strategy shifts the emphasis to the private market, stating that "Israel intends to expand the activities of its centers of excellence and laboratories in collaboration with the broader ecosystem, making them more accessible to the private sector". The development of human capital in the cyber field remains a continuing objective in the new strategy.

The previous document supported cooperation in the international arena by promoting collaborations to raise the level of national and global cyber security and assisting partner countries in strengthening their own national capabilities. In the new strategy, this effort is more focused on security needs. It includes the deepening of ties with "leading partners" and more closely defines the need for early warning and enforcement. Assistance to friendly countries is focused on times of "national cyber crisis".

The main points of the National Cyber Directorate for 2025 appear in the work plan of government ministries and units of authority, which was published in April 2025 after the transfer of the state budget. The five principles of the work plan and the objectives defined for their implementation do not yet reflect the new strategy. This is despite the fact that the way the objectives and projects for their implementation are defined largely overlaps with the strategy that was

completed at the same time. Examples of new strategy objectives that are not defined in the work plan include motivating businesses to strengthen their security (objective 1.3 in the strategy), maintaining zero significant damage to critical infrastructure (objective 2.1), and effective national digital crisis management (objective 5.2).

A useful document for comparison is the United States Cyber Strategy of March 2023, which was released during the Biden administration. That strategy was focused, as is the updated Israeli strategy, on the processes required to secure cyberspace. The first principle of the American document was to define the path to immunity in cyberspace by balancing responsibility for its protection and incentives for long-term investment. The administration threw its weight behind several fundamental changes: regulating and deepening the defense of critical infrastructure within the government and with business entities operating in these areas; addressing threat actors by disrupting and dismantling them; and shaping market forces to drive security and resilience by imposing responsibility and providing incentives to technology giants while rebalancing responsibility between infrastructure service managers and end-user entities.

One sees a thematic overlap with the Israeli strategy and response to parallel concerns, indicating a similar analysis. However, unlike Israel, the American focus is on using government powers in terms of regulation and resources to bring about an aggressive correction of the situation. The Israeli strategy, which, due to constraints I will address below, strives more for the exploitation of "soft power" in the creation of coalitions and collaborations and less for the aggressive use of the "hard power" of legislation and resources.

The additional foundations of the American strategy are investing in a resilient future and forging international partnerships. These are analyzed from the perspective of a technological and political superpower that leads global processes. In this the US differs from Israel, which is a part of global processes rather than their leader and is therefore limited in its ability to influence them.

Another principle of the American strategy was the continuity of effort within the framework of existing policy. Creating a continuum between existing processes and a new strategy is a desirable move and one that Israel adopted in its own document. It should be noted that the Trump administration's moves

to ratchet up government efficiency (DOGE) have actually changed key components in the ability to implement this document. One example is the deep cuts to the National Cyber Security Agency (CISA) and the National Institute of Standards and Technology (NIST), which form the basis for best practices in cyber security processes worldwide.

The content of the new strategy

Israel's new strategy is a comprehensive and clear document that contains the required efforts in the field of cyber security as they are currently accepted worldwide. A number of key insights emerge from it.

First of all, the document **defines the national vision of cyber security** as "a trustworthy, reliable and safe digital space". It places cyber security in its natural and proper place as a means of ensuring core national security in all its manifestations, including infrastructure, the economy, and society. While the definition lacks reference to adaptation with a forward-looking perspective due to the rapid pace of change in the digital field, its authors stress that it is written with a three-year horizon (until 2028) and state the need for dynamic response.

The strategy includes **two issues that are not part of the core of conventional cyber security:** creating a sharper and more resilient public consciousness of malicious foreign influence (objective 3.4) and a national plan for secure digital identification (objective 1.4). The latter refers to the National Cyber Directorate's responsibility for biometric identification and reflects the inclusion of this issue in the American strategy. The presence of these issues raises the question of what the whole of national cyber security really is and whether other aspects should be added to the principles at the national level (for example, defining the migration of government ministries to the public cloud as a key component of the national cyber security concept or addressing national encryption policy).

The document identifies a **difference between the network and the supply chain approach** to cyber security. It states that "users and owners of digital assets in cyberspace do not control production stages and operational aspects… a fact that emphasizes the need for regulating responsibility at the national level". This expresses a basic understanding that the security envelope for

organizations must be much broader than controlling the supply chain or third parties (the document uses the phrase: "technological supply network).

The new strategy also takes a **proactive approach to cyber crises**. It stresses the need to be well prepared and articulates what it calls "effective national digital crisis management", a concept that includes the principles of active security and resilience and crisis preparedness. However, unlike the practical and legal discussion currently developing around the world (see the US and Japan) under the heading of a "proactive approach" regarding the integration of the offensive dimension, at both the national and organizational levels, in response to cyber incidents, the Israeli document obscures the national response under the heading "response to attackers" (objective 6.1). It can be assumed that this section refers to national actions carried out against attackers and the countries or organizations that operate them, as has been attributed to Israel in recent years. This is the beginning of a discussion, not its end. Another response issue where the document takes a significant step is its clear statement that "the Government of Israel advocates not paying a ransom in order to thwart an attacker's intent".

Israel, unlike the US in its limited ability to influence, deals with global technology giants by "developing "**strategic partnerships with domestic and global technology companies**" (objective 7.1). As far as the "technology supply network" (i.e., "the key nodes in the provision of ICT services") is concerned, up-to-date mapping and "across-the-board resilience" (objective 3.2) are required.

A primary objective of the strategy is **the raising of awareness and literacy against cyber threats** (objective 1.1). This sends a clear message that cyber security begins with understanding the challenge and the role of each body in addressing it.

In several places, the document chooses the **soft path of cooperation over enforcement**. For example, a direction of action for a unified national system for voluntary reporting is defined within objective 1.2. In reference to privacy protection within the framework of "securing information assets holistically" (objective 3.3), the document defines a need for a "complementary perspective" alongside that of the Privacy Security Authority, mainly in terms of the ability

to draw insights from an aggregate of unclassified information. This shows an understanding that imposing overly strict reporting duties and enforcement actions are not the best response to cyber security challenges.

In two places, the new strategy document refers to **lessons learned from the Iron Swords War**. In "avoiding and preparing for digital surprises' (objective 5.1), it states: "The human factor plays a critical role both in the advent of an unpleasant surprise and in management of the subsequent crisis. Cognitive and psychological biases tend to underestimate the plausibility of a strategic surprise...", so compensatory mechanisms are required to deal with such a situation. Within the framework of "development of skilled human capital" (objective 8.3), it is determined that "Israel will work to break the 'juniors barrier' - the lack of initial experience… by encouraging the employment of wounded veterans from the Iron Swords conflict… in entry-level roles in government and industry...". It is impossible to overstate how worthy and correct this effort is.

Recommendations for implementation

The strategy will be measured, as ever, by its implementation. As written, it should become the basis for the work plan of the INCD and other national cyber security-related bodies in the coming years. Four key recommendations can be identified in the implementation process:

A. **Building the strengths of the INCD:** The strategy places the INCD at the center of a network of government and national collaborations. The strength of the INCD is not built on legislation and regulation that allow it significant enforcement capabilities (except in the vital area of critical infrastructure) but rather on the professional and operational strengths it brings to the table. In this respect, it is similar to the Mossad, which is also responsible for activities within a specific domain (in its case, abroad), even though the legal powers for its operations are limited. In the Mossad's case, the organization is built on the unique and creative strengths of knowledge and operations it has compiled over the past 70 years, and it brings these advantages into dialogue with other government entities operating abroad. This should be the approach of the INCD. It must build unique capabilities, both independently and in

collaboration, that provide substantial added value to all parties. This will form the basis for its claim to be present in every matter related to national cyber security.

B. **The limits of security ("what not to do"):** One challenge in translating a strategy into a work plan is to narrow down the objectives. Phrases like "extensive public awareness education" (objective 1.1), "providing better access to basic cybersecurity tools and services" (objective 1.2), "maintain high levels of security for governmental ICT systems" (objective 2.3), a "cyber dome" that includes "a whole host of advanced capabilities and offers an across-the-board solution for a swifter response" (objective 4.2), and "embed principles for building an economy that is more resilient to digital crisis" (objective 5.1) all require clarification to establish an unambiguous order of priorities in the face of a defined cyber threat profile (CTP).
C. **The proactive approach:** The world's leading countries are converging on decisions that define the boundaries of their proactive approach, which can include legal action in the international arena, remote damage to an attacker's infrastructure, and the use of military force against or because of cyber threats. The State of Israel should hold a principled discussion on this issue and establish a clear policy, even if this is done behind closed doors.
D. **Quantum computing:** The current strategy overlooks the issue of quantum computing, which is somewhat justified given its focus on the next three years. However, quantum technology must be discussed now, if only because of its impact on the issue of encryption, which is a key component of cyber security.

The great test of the new strategy document will be its focused and prioritized implementation, with an emphasis on the building of the INCD's strengths as the generating core of national cyber security. Israel's cyber security strategy document should be updated every three years, not every eight.

Col. (res.) Shay Shabtai is a senior researcher at the BESA Center and an expert in national security, strategic planning, and strategic communication. He is a cyber security strategist and a consultant to leading companies in Israel.