BESA
The Begin-Sadat Center
for Strategic Studies
Bar-Ilan University

National Cyber Strategy: Issues for Discussion

Shay Shabtai

Mideast Security and Policy Studies No. 203

THE BEGIN-SADAT CENTER FOR STRATEGIC STUDIES
BAR-ILAN UNIVERSITY
Mideast Security and Policy Studies No. 203

National Cyber Strategy: Issues for Discussion

Shay Shabtai

National Cyber Strategy: Issues for Discussion

Shay Shabtai

© The Begin-Sadat Center for Strategic Studies
Bar-Ilan University
Ramat Gan 5290002 Israel
Tel. 972-3-5318959
Fax. 972-3-5359195
office@besacenter.org
www.besacenter.org

ISSN 0793-1042
July 2024

Cover image: Shutterstock

The Begin-Sadat (BESA) Center for Strategic Studies

The Begin-Sadat Center for Strategic Studies is an independent, non-partisan think tank conducting policy-relevant research on Middle Eastern and global strategic affairs, particularly as they relate to the national security and foreign policy of Israel and regional peace and stability. It is named in memory of Menachem Begin and Anwar Sadat, whose efforts in pursuing peace laid the cornerstone for conflict resolution in the Middle East.

BESA Perspectives are short pieces on timely and fundamental Israeli, Middle Eastern, and global issues. Mideast Security and Policy Studies serve as a forum for publication or re-publication of research conducted by BESA associates. Colloquia on Strategy and Diplomacy summarize the papers delivered at conferences and seminars held by the Center for the academic, military, official, and general publics. In sponsoring these discussions, the BESA Center aims to stimulate public debate on, and consideration of, contending approaches to problems of peace and war in the Middle East. The Policy Memorandum series consists of policy-oriented papers. Publication of a work by BESA signifies that it is deemed worthy of public consideration but does not imply endorsement of the author's views or conclusions. A list of recent BESA Center publications can be found at the end of this booklet.

Executive Board

Prof. Amnon Albeck, Prof. Gil S. Epstein, Prof. Eitan Shamir, Prof. Rami Ginat, Prof. Jonathan Rynhold, Prof. Joshua Teitelbaum

Research Staff

BESA Center Director: Prof.Eitan Shamir

Research Associates: Dr. Shay Attias, Prof. Efrat Aviv, Lt. Col. (res.) Dr. Shaul Bartal, Dr. Yael Bloch-Elkon, Dr. Ziv Bohrer, Col. (res.) Dr. Raphael Bouchnik-Chen, Brig. Gen. (res.) Dr. Moni Chorev, Dr. Netanel Flamer, Prof. Jonathan Fox, Maj. Gen. (res.) Gershon Hacohen, Dr. Eado Hecht, Prof. Efraim Karsh, Prof. Udi Lebel, Dr. Alon Levkowitz, Cdr. David A. Levy, Dr. Joseph Mann, Brig. Gen. (res.) Eran Ortal, Navy Commander (ret.) Eyal Pinko, Dr. Elai Rettig, Dr. Elisheva Rosman, Col. (res.) Dr. Uzi Rubin, Prof. Jonathan Rynhold, Prof. Shmuel Sandler, Mr. Ran Segev, Col. (res.) Shay Shabtai, Lt. Col. (res.) Dr. Dany Shoham, Prof. Shlomo Shpiro, Prof. Joshua Teitelbaum.

Operations and Finance Manager: Alona Briner
English Publications Editor: Judith Levy
Digital Media Marketing Manager: Shany Shriki

National Cyber Strategy: Issues for Discussion

Col. (res.) Shay Shabtai

EXECUTIVE SUMMARY

This paper raises essential issues for discussion regarding the design of Israel's national cyber strategy. It deals with aspects related to the promotion of national cyber security and the improvement of national resilience and the private sector's ability to cope with major attacks that have security, economic and social impact.

The paper concentrates on what the author considers to be the key issues. It neither pretends nor aims to encompass all the elements involved in formulating a national cyber security strategy. It is intended to point out the complexity of the issues concerned and create a basis for deepening discussions about them. In the service of the discourse, it does not contain decisive or unequivocal recommendations. Nor does it deal with the offensive component, which is a fundamental component of an overall national cyber strategy.

I would like to thank Ram Levy, CEO, and Deborah Housen-Couriel, CLO, of Konfidas; Lior Kalev, head of cyber security Partner - Cyber Risk Services and Innovation Leader at Deloitte Israel; Guy Halfon, CEO of Rescana; and Dalit Caspi-Shachner, the cyber security strategy leader of Bank Hapoalim for their smart comments on paper. Nevertheless, the contents of the paper are solely the responsibility of the author. The Hebrew version was presented to the Israeli National Cyber Directorate (INCD).

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.

Introduction

This paper is structured to present the key issues concerned with the formulation of a national cyber strategy in a "top-down" order, from the national strategy level to cyber security efforts. It addresses the following five issues:

Issue 1: The *strategic context* of national cyber security and how it should connect to the national strategy; the strategy, policy and doctrine of national security; and the national computing policy.

Issue 2: The *Cyber Threat Profile (CTP)* to which the National Cyber Security Strategy should direct the response.

Issue 3: The *scope* of the discussion, the *goals* of the strategy and the *connection* between them and cyber security circles and levels of national cyber security.

Issue 4: The *complexity* of arranging the place of the cyber security echelon within the government sector and vis-à-vis the civil-business sector as a derivative of the strategic concept.

Issue 5: Raises and analyzes several key efforts in the field of cyber security.

Summary of recommendations

One of the goals of the annual work plan of the Israel National Cyber Directorate (INCD) for 2023 – halted by the outbreak of the Iron Swords War - was to formulate the country's national cyber security strategy and build a multi-year work plan. The process was thorough and lasted many months.

Below are presented recommendations that address the strategic context, the national Cyber Threat Profile (CTP), which refers to response efforts, national cyber security goals, the roles and responsibilities of national-level cyber security organs within the government sector and vis-à-vis the civilian sector, and key cyber security efforts. Each recommendation will be examined in greater depth later in the paper.

Issue 1 - The "puzzle": Cyber security strategy as part of national strategy: How can a national cyber security strategy and policy be defined in the absence of national level strategy and policy papers that determine long-term principles and goals in an overall national vision and in areas that affect cyber security, including national security, internal security, foreign policy, and national IT?

Recommendation: National cyber strategy should focus as much as possible on the core aspects of cyber security and refrain from promoting non officially approved "national goals" that were not defined within broad national thinking or validated by official decisions.

Sub-issue 1a - Cyber and national security doctrine: Is it right to create national security doctrine principles for the cyber domain other than the traditional ones (transferring war to the enemy's territory, deterrence, early warning, defense, decisive decision)?

Recommendation: Caution should be exercised in adopting principles of national security doctrine that are much less relevant to cyber security.

Sub-issue 1b - Influence of national IT policy on cyber security: What is the right equilibrium of cyber security efforts between future projects whose purpose is to develop concepts, architectures and means of protecting future technologies, even if national projects that are part of the IT vision are not realized at the end; and present concerns about the implementation of current projects?

Recommendation: It is necessary to identify key issues and areas within the national IT framework in which there is a strong need to build long-term response processes and for them alone build preliminary national preparedness.

Issue 2 - Prioritization of the national Cyber Threat Profile (CTP): Should the national CTP, which is the basis for determining security efforts, identify economically motivated criminal APTs attack as a top-level threat? Are Russian and Chinese state threats no less and possibly even more important than the Iranian threat?

Recommendation: In determining the national CTP, it is advised to give a lower priority to broad strategic considerations like the overall

Iranian threat and to focus on identifying and ranking cyber threats that pose the greatest potential to damage national, governmental, and business resources.

Issue 3 - Focus of national cyber security goals: What is the right balance in the definition of national goals and the principles of their implementation between focusing on cyber security efforts and promoting national economic and security ventures in cyber?

Recommendation: In defining national goals in the field of cyber security, it is advised to refer to the unresolved tension between a broad vision of global leadership and Israel's real-life cyber security challenges and prioritize the practical needs. Only after these needs have been met would it be appropriate to consider diverting residual resources toward efforts that are not at the core of security. These core needs can, for example, be in the short and medium term the migration of national and business entities to the national cloud and in the medium and long term the ability to establish isolated national environments within public resources such as the cloud or supercomputing.

Sub-issue 3a - Cyber security "circles": Should national cyber security be limited to dealing only with critical infrastructure and maintain a general standard of security for the rest of the economy, or should it deepen defensive efforts to all the different "circles": (1) international corporations, (2) critical national infrastructure, (3) major Israeli IT suppliers, (4) large regulated companies, and (5) SMBs, SOHOs and the general public? Should it tailor solutions to all "circles" (for example, a "national umbrella" when dealing with international corporations that are a major part of the Israeli economy supply chain)?

Recommendation: As part of the strategic process, it would be advisable to map the issues in which governmental and business entities in different "circles" have trouble providing an independent defensive response. The state can make a significant contribution to closing those gaps. It would be wise to prioritize the response of the national process to these issues.

Issue 4 - The basic approach of the INCD: What is the optimal utilization of models of governmental organizations (security, law enforcement, internal government authority, regulatory body, general information, and direction) that the INCD can adopt in a way that will allow it to fulfill its duties in an optimal way at different levels of response and in all "circles"? Would it not be advisable to promote, with a long-term view, the integration of the INCD into a government ministry other than the Prime Minister's office that would give it attention and resources it cannot currently receive?

Recommendation: In decisions about the characteristics of the INCD and its subordination, it is advised to consider the most effective means of influence of government bodies on other government offices and on the business sector. It is also advised that the INCD and the cyber security units in the government ministries focus on security and refrain from operational and law enforcement aspects handled by other organizations (intelligence, police, privacy protection, etc.). A combination between internal government authority and a regulatory body would likely be the most effective.

Issue 4a – Cyber security in the government sector: How can the aspects of cyber security be promoted in additional government ministries beyond those that have already made the leap (Ministry of Energy and Infrastructure, Ministry of Communications, etc.), and in which cyber security should receive more attention and resources beyond those currently provided (e.g., Ministry of Health, Ministry of Transportation, Ministry of the Interior, Ministry of Education)?

Recommendation: Increasing the involvement of the INCD – based on clear regulation of its mission and roles - and enhancing security activity in all government ministries and organizations should be a central goal in the strategy.

Issue 4B – Cyber security in the business sector: How can national cyber security strategy lead to optimal cooperation of the INCD and other governmental cyber security units with the business sector? How can this cooperation optimize security processes like a national approach to supply-chain cyber security, regulation that promotes positive change, a national "security umbrella" to protect private businesses, handling the cyber security manpower shortage, cooperating with cyber security services companies, etc.?

Recommendation: The solution of horizontal cyber security difficulties – for example, the lack of skilled cyber security personnel - should be a central engine in the relationship between the national cyber security apparatuses and the civilian ecosystem.

Issue 5 - Efforts in the field of national cyber security: To what extent and in what form should the INCD and other governmental cyber security units engage in cyber security efforts?

Recommendation: It is advised to:

a. Expand the national effort of training skilled personnel for cyber security for government ministries and agencies and the civilian sector and make regulation of this effort more flexible.

b. Limit and reduce national support efforts and allocated resources to cyber security R&D.

c. Focus and delineate the Gov2Gov international cooperation effort according to stricter priorities with flexibility for opportunities. This effort should include the capability to support friendly countries under attack.

d. Adapt internationally recognized cyber security best practices to the unique characteristics of Israeli culture and conduct.

e. Carry out national processes to adjust compensation mechanisms so they cover damage resulting from cyber-attacks by state actors and terrorist organizations.

Elaboration of analysis and recommendations

Issue 1 - "The Puzzle": Cyber security strategy as part of overall national policy

Israel's national cyber security strategy and policy does not stand on its own. In fact, it constitutes the fourth layer of the national strategy and policy. Its position on the ladder can be described as follows:

The first layer is the national strategy, within the framework of which the government sets national goals with an aggregate vision emphasizing political-security, economic-social and infrastructural concerns. Israel has no formally written national strategy. From time to time, fundamental work is done in core areas, and it is partially implemented. There have been several attempts by research institutions to create a comprehensive master document, but the overall national action is not based on a coherent strategy.

Significant progress in this regard was seen in the distribution, most recently in July 2023, of the main points of the annual work plans of the various government ministries and trust units, which at least provides a good mapping of the goals they are working to promote in the absence of a national strategy.

The second layer is strategy in the fields of national security and socio-economics. The national security strategy is the basic document of the elected political level. It analyzes the basic data and the broad context of national existence - political, economic, demographic, social, historical, cultural, political and security-military. It then defines, on the basis of the worldview of the political echelon, the national goals (ends); the required national abilities (means); and the principle ways of action (ways) that allow the realization of the national goals.

In many countries in the world it is expected, sometimes by law, that the incoming administration publish a national strategy or national security white paper. There is no such document in Israel. Furthermore, in Israel, the term “Security Concept” has taken root, an approach that involves a partial discussion of each of the levels of national security: strategy, theory and policy. As a result, an orderly and official discussion does not take place on national security strategy. An attempt to enshrine in legislation the powers of the National Security Headquarters in this area did not lead to a substantial change in the situation.

At the level of national economic strategy, there has been, since 2006, a formal body - The National Economic Council - whose role is to “formulate and lead strategic processes for the advancement of the

Israeli economy and society." This body addresses a great deal of national strategy components and builds a socio-economic strategic situation assessment. That assessment is not, however, incorporated into a national strategy document at the end of the process.

The third layer is National Security Doctrine and Policy documents:

1. The **doctrine of national security**, known in other countries of the world as National Security Doctrine or National Security Guidance, is the basic document of the security echelon, and in essence is not immediately affected by the worldview of the elected political echelon. It defines the basic conventions, principles and concepts underpinning the ways of dealing with security-military challenges. Israel has an agreed-upon but informal national security doctrine, and I will detail its cyber connection below.

The theory behind national security *doctrine* is The National Security *Policy*, known in other countries as National Security Policy or National Security Review. This is a document that delineates the principles of operation of the political-security echelon based on combining the principles of the Strategy and the Doctrine. It expresses a contemporary national assessment of the prevailing situation and the current directives of the political echelon on the issues at hand. This document also does not exist in Israel, but the annual national assessment of the National Security Council (NSC) can be considered an equivalent.

2. **"Foreign policy"** is a general term for the group of goals that define the way in which the country behaves in relation to other countries of the world. Israel does not have a document detailing its foreign policy as a derivative of national security strategy and national security policy. However, the chapter of the Ministry of Foreign Affairs in the main document of the work plans can be considered a type of foreign policy document, even though foreign relations activities are managed by government ministries and other state organizations (the Mossad, the IDF) and are not weighted into this document.

3. **Internal security policy** is also supposed to be contained in a fundamental document that defines the government's principles of action regarding the maintenance of public security, proper governance and law and order. Here, the chapter of the Ministry of National Security in the main document of the work plans serves as a type of internal security policy document, though it does not cover all the government's internal security efforts.

4. **National IT policy** is the state's overall outlook on how to develop, integrate and exploit computing capabilities to promote advanced infrastructure and operational capabilities. Israel has progressed by leaps and bounds in this area over the past two decades, and during the coming year, the National Digital Array intends to formulate "a comprehensive strategy in all areas of the array's activity, starting with the design of an up-to-date national digital strategy and then a strategy in the worlds of government information systems, data and artificial intelligence in the public sector, a government transition strategy to the cloud, government cyber strategy and advanced service strategy." To this can be added the objectives of the Ministry of Innovation, Science and Technology in the fields of artificial intelligence and quantum technologies. More on that below.

These are the levels of national strategy and policy that should be expressed in final and approved documents, which are above national cyber security strategy and policy. From below, strategy and policy are built on the basis of situational assessments regarding technological change and the Cyber Threat Profile (CTP), which will be expanded upon later in the paper.

National cyber security strategy and policy can partially rely on the national basic documents alone. A national digital strategy, which is a critical component in determining the principles of cyber security, is to be written in the near future. The main document of the government's work plans can finalize the informal elements of the security doctrine and the NSC's situational assessment can be considered a national security policy.

It is important that the INCD be based on these documents when determining strategy and policy. Determining them on the basis of other anchors could lead to the establishment of goals and principles that are not connected to national needs. (See the discussion below on the focus of national goals.)

On the negative side, essential layers that should form the basis of national cyber security strategy and policy are missing. This is especially noticeable in the long-term view, as will be explained below. It is possible, perhaps, to establish reasonable working assumptions mainly with a long-term view, but take into account that these must be re-examined frequently - at least once a year and given developments in national fundamental determinations.

The issue for discussion: How to define and prioritize a national cyber security strategy and policy in the absence of strategy and policy documents that determine long-term principles in an overall national vision and in influential areas such as national security, internal security, foreign policy and the national computing concept?

Recommendation: National efforts in the field of cyber that are not connected to an overall national strategy cause problems arising from the potential to create biases in the way the cyber ecosystem is built as part of the national complex. Thus, for example, it can be argued that there is an excessive focus on the Israeli cyber security industry that makes it difficult to promote sectors that may be more critical to the national strategy. Therefore, it is desirable that national cyber strategy focus as much as possible (see below for national cyber security goals) on the core aspects of cyber security and refrain from promoting "national goals" that have not been defined in the framework of national thinking and validated in official decisions. A discussion of this question can also be relevant to other national efforts.

Sub-issue 1a - Cyber and the national security doctrine

Israel has an agreed-upon but informal national security doctrine. Designed by David Ben-Gurion, it provided an answer to Israel's basic inferiority, in terms of population and resources, between itself and its hostile neighbors of the time. At the center is the difficulty of putting up a military force equivalent in strength to that of the Arab states. Therefore, at the base of the doctrine is the desire to postpone military conflicts as much as possible and conduct them only if necessary, so as to concentrate the country's full capabilities in order to bring about a decision when faced with a significant state military threat; i.e., a threat to invade Israel's territory.

Israel's original security doctrine – which, as noted, is aimed at a conventional military threat – has three main principles: defensive strategy and offensive action, the "People's Army," and the 'Security Triangle'.

Defensive strategy and offensive action: Ben-Gurion formulated a basic principle according to which the Israeli military strategy is defensive; that is, reactive to threats partly to preserve international support. However, it is manifested in offensive action that moves the war to the opponent's territory as early as possible so the main battlefield is not inside Israel's small territory.

"The People's Army": The IDF was based on conscription, which allowed it to maintain a relatively small regular force to dealt with routine security tasks and prepare the IDF for war. If necessary, the conscripted soldier was expected to defend the country in the first stages of war. Beyond the nucleus of regular soldiers, a large reserve army was built that maintained war-readiness. If ordered, the reserves could mobilize relatively quickly and turn the IDF into an army big enough to deal with a military coalition.

The "security triangle": The need to postpone conflict as much as possible and resolve conflicts that do erupt as quickly as possible led to the formulation of three basic concepts. They were originally aimed at state military threats, but were updated along the way - including as part of the Meridor Committee discussions - to respond to other types of threat:

1. **Deterrence:** Israel will maintain clear superiority in capabilities over its potential adversaries and will transmit determination in a way

that will lead decision makers on the other side to hesitate to enter into conflict with it. The concept of deterrence was expanded later to make it relevant to the fight against terrorism.

2. **Early Warning:** Israel will detect changes in the adversary's intentions and the readiness of their military forces and prepare for a confrontation in sufficient time to mobilize the full strength of the IDF, with an emphasis on the reserve army. The field of early warning has been expanded in recent decades to all types of possible threat. This expansion has led to a significant increase in responsibility for the intelligence community.

3. **Decision:** In view of the lack of operational depth in the territory of the State of Israel, the IDF will, as early as possible (preferably at the beginning of the conflict and even on its own initiative; i.e., "preventive war", "preventive strike"), conduct an attack that moves the fighting to the enemy's territory and sets the conditions for a relatively long period of peace. In recent decades, attempts have been made to apply the concept of decision to other contexts - WMD, terrorism - but this is complex and impractical.

In the deliberations of the Meridor Committee, which operated between 2003 and 2006, it was decided that beyond expanding the canvas of the existing concepts, a fourth fundamental concept should be added to the "security triangle": "defense". This principle is anchored in security theory. Israel invests a significant portion of its budget and security efforts on passive defense. To these can be attached a security system, both public and private, of wide dimensions. This defense concept adds to passive defensive tools by providing offensive tools aimed at thwarting steep trajectory shooting or terrorist attacks below the broad escalation threshold.

The short review above is Israel's security doctrine. The basic conditions of the cyber field are completely different from those that characterized Israel's security in the 1980s. The cyber medium disrupts concepts of boundaries and sovereignty that are at the heart of the original theory, requiring these additions:

1. A distinct *technological advantage* in the cyber field over the Middle Eastern countries in the cyber field.

2. A distinct *resource advantage* in the cyber field over the Middle Eastern countries.

3. A cyber security capability to deal with significant attacks without the need to "transfer the war to the enemy's territory."

4. Cooperation rather than rivalry in the cyber field with key countries in the region, with an emphasis on the Abraham Accords countries.

These basic conditions in the cyber field raise a big question mark about the relevance to cyber of the principles of security theory. Foreign publications attribute to Israel the execution of retaliatory cyber-attacks in Iran. Chief of Staff Major General Aviv Kochavi stated in May 2020, amid reports of a cyber-attack attributed to Israel against an Iranian port, that "we will continue to act with diverse tools." If Israel does carry out cyber-attacks on Iran for the purposes of "deterrence" and "decision," the question arises whether it is correct to apply the elements of Israel's traditional security theory to this field.

Contrary to the basic approach of traditional security doctrine, Israeli power in cyberspace allows Israel to, for example, focus on defending against the opponent and thwarting most of its attacks, or at the very least greatly reducing its operational effects. In this way, it allows for deterrence by denial without the need to invest resources in counterattacks for purposes of "punishment" or "decision." It may be more appropriate to respond to Iranian cyber attacks through diplomatic and legal moves that would isolate that country and make it pay a strategic price for its aggression than reacting with an offensive cyber action. Added to this is the fact, as will be discussed below with reference to the attribution threat, that threats to Israel in the cyber field come from actors for whom security theory is even less relevant.

The issue for discussion: Is it correct in the cyber field to create national security doctrine principles beyond the traditional ones and as a result change the mix of response to threats?

Recommendation: As a preliminary step to the process of defining dedicated national security doctrine principles in the cyber field, caution should be exercised in adopting principles that are not specific to cyber security such as early warning and protection. In this framework, questions can be raised about the relevance of the concepts of deterrence to the cyber field. Discussion of this question can also be relevant to other areas in the field of national security.

Sub-issue 1b - Connecting cyber security to national computing policy

The State of Israel has made considerable progress in recent decades in the field of national computing policy: building the government site (egov), establishing the National Digital System and the National Cloud Project (Nimbus), progress in information and artificial intelligence applications in government offices, promotion of the deployment of advanced communication infrastructure, super and quantum computing, and more. All of these indicate a desire to move Israel's computing infrastructure to an advanced, world-leading position.

However, over the years, these ambitious plans encountered difficulties in implementation and were either reduced or had their implementation spread out over many years. Also, the actual implementation differs, sometimes in essence, from the original plans. Thus, for example, a review by the state auditor on preparations for the establishment of a central cloud stated that "in 2019, the government invested in cloud computing less than 1 percent of its total investment in ICT, compared to 8% in the world." As for the status of the Nimbus project, the report stated:

> The Nimbus project is a multi-year project that began in 2019 and is designed to provide a comprehensive solution to the issue of providing cloud services to government offices. The project consists of four layers that make up the central tender of the Government Procurement Administration. During 2020, tenders were published for the first layer (providing cloud services) and the second layer (Center of Excellence in Cloud Computing) of the tender, and during February 2021 a tender was published for the third layer (modernization and migration services). A tender for the fourth layer (monitoring

> and optimization services) has not yet been published, and no estimated date has been set for its publication.

As for the cyber security aspects of the use of the cloud, the report said that:

> Despite a dedicated directive from the director of the cyber protection unit in the government…which states that any system that operates in the cloud environment requires the approval of the advisory committee on the issue of transferring information and computing applications to the public cloud environment... From the answers of 42 ministries to the questionnaire distributed by the state comptroller's office, it appears that in these offices about 10 systems operate in a cloud environment without the approval of the advisory committee being sought. Operating such systems in a cloud environment without the committee examining whether there is any reason to approve them may lead to the realization of information security risks involved in operating these systems.

Also, in the field of supercomputing, which is essential, among other things, for promoting the national program for artificial intelligence (AI), it was reported that the national supercomputer project from 2020 was split into three smaller projects: use of supercomputers through the cloud services of large international providers as part of the Nimbus project, participation in a network project consisting of the supercomputers of the European Union as part of the Digital Europe initiative, and the establishment of a supercomputer and artificial intelligence laboratory. One of the proposals submitted under this project is by Nvidia, the largest manufacturer of AI servers in the world, but it did not wait for the national project. In mid-2023, it launched the supercomputer Israel-1, stating that it will be used for research and development and later for providing services to the private sector.

In the field of quantum there is a declaration of intent in the form of the design of a central national plan, but it seems that progress in this field is still decentralized around the initiatives of academic institutions and business organizations and is neither broad nor deep enough to meet the size of the challenge.

This situation, in which key components of a national computing policy exist but are implemented only partially and take much longer than planned, creates a dilemma for national cyber security. On the one hand, projects of this magnitude must be accompanied by aspects of protection from the examination and pre-project stages. In order to build a protection architecture for such extensive and advanced computing infrastructures, for some of whose security aspects there are no relevant protection technologies currently available on the market, a continuous and expensive process of learning, consultation and even reliance on external experts, planning and timely implementation of the security aspects is required. The cyber security of major national projects has been compromised in the past by the absence of such a process. On the other hand, the gradual and continuous implementation of projects and the need to adapt security on the fly to updated architectures mean an investment - sometimes considerable - of additional resources.

The issue for discussion: Connecting national cyber security to national computing policy, what should be the response mix of cyber security between processes and projects that aim to build concepts, architectures and means to protect future technologies, even if national projects are not realized in the end according to the vision?

Recommendation: Key issues and areas must be identified within the framework of the national projects, where there is a great need for serious thought on long-term response building processes and ways to carry out preliminary national preparations. Core short- and medium-term needs can include the migration of national and business entities to the national cloud, and in the medium- to long term, the ability to establish isolated national environments within public resources like the cloud or supercomputing.

Issue 2 - Prioritizing the Cyber Threat Profile (CTP)

First, a brief methodological introduction. The Cyber Threat Profile (CTP) is not a kind of “intelligence assessment” of the total number of possible threats, in this case in the cyber field, to the State of Israel.

Nor is it an analysis of all existing risks. The CTP is a form of "super-analysis" - the forest, not the trees - aimed at enabling decision makers to make informed decisions about national cyber security strategy.

The CTP defines, on the basis of the national strategy, the country's main assets and the extent to which damage to those assets inflicted by a hostile element would weaken the state. The first question to be asked, therefore, is: What is important to us?

Determination of the CTP involves assessing the types of possible adversaries, their capabilities, and their objectives, as well as mapping significant events (not simply a list of "bad things") that can happen. The state's current level of security is assessed - that is, the protection measures and processes that are currently implemented or set to mature in the near future, and what level of security they provide. If we did not take into account the existing level of security, the threat would be absolute (in the language of risk management, the realization of the "root risk") – in other words, any cyber amateur could cut off the electricity in the State of Israel because nothing would stand in his way. This is of course not the case.

The result is a description of the "big things": the significant threats to the country in the cyber field. This allows senior decision makers to decide what is important to protect, what the priorities are, how many resources should be invested, and which protection efforts should be focused on. If this process is not gone through, it is difficult for the national decision makers to understand the cyber threat. Going too much into technical details creates a distance between the decision makers and the professionals doing the assessments, particularly as cyber is inherently difficult to digest.

The current threat picture raises a major dilemma. In an article in *Haaretz* (July 12, 2023), the head of the INCD, Gabi Portnoy, defined Iran as the main threat. According to the article, most of the attacks on Israel come from Iran, where 15 hacker groups operated in the past year compared to five the year before. The most severe attack was on the Technion. Iran is also helping Hezbollah and Hamas upgrade their cyber security and attack capabilities. But no significant information seems to have been released. Portnoy notes that other countries, including China and Russia, are cyber-attacking Israel as well, but are doing it mainly to gather information rather than to cause damage to institutions and entities.

The State of Israel rates the threat from Iran and its partners as the most severe. This is a security perspective that considers the national cyber threat to come first and foremost from enemy states or entities, not from superpowers, and with less emphasis on civilian cyber threats. This ordering of priorities seems to have affected the Israeli response, as reflected by the attribution by Tehran of cyber incidents within Iran to response attacks by Israel.

But are they in fact the most significant threats?

The main cyber threat to advanced countries is from advanced criminal elements that conduct their attacks in the form of ransom and extortion. The most vulnerable entities in recent years - especially since the Covid-19 pandemic – were large civil organizations that were hacked and shut down. This caused damage to critical infrastructures like the gas supply on the American east coast (Colonial Pipeline, May 2021), major medical institutions (a hospital near Paris, August 2022) and damage at the national level (government of Costa Rica, April 2022). Some of these criminal gangs have national motivations, but the essence of the attacks is opportunistic. Organizations are attacked by these criminal elements on the basis of technological accessibility and business capability.

The issue for discussion: Should the CTP, which is the basis for determining the country's security efforts, prioritize economic attack descriptors of sophisticated cybercrime actors? Should Israel consider powerful threats from China and Russia significant, possibly even more than the Iranian threat?

A different composition of the CTP can have an impact on decisions regarding the response mix to those threats: Where to focus intelligence collection? How to cultivate commercial cyber intelligence relevant to the threat mix? How should protection, monitoring and warning efforts be distributed? Against which threats is the national response focused in terms of active defense (cyber attacks for preventive purposes) and deterrence?

Recommendation: In determining the national CTP for cyber security, Israel should give a lower priority to broad strategic considerations - for example, who the threat factors are in other dimensions – and instead focus on identifying and ranking the factors that have the potential to cause major cyber damage to national government and civilian capabilities.

Issue 3 - Focusing national objectives in the field of cyber security

The existing cyber security strategy document from 2017 defines the cyber vision of the State of Israel thus: "The State of Israel will be a leading state in harnessing the cyberspace for the benefit of its economic growth, social welfare and national security." This wording is based on the recommendations of the national cyber project from 2011. Israel's cyber vision will not explicitly include national cyber security until the current version is changed.

The concept of action to realize the vision, which can perhaps be defined as the State of Israel's cyber security goals, includes three components:

1. **Business resilience:** "The ability of organizations in the business of inter-organizational and business processes to continue their activities while under cyber threat." This component is promoted through direct and indirect regulation of organizations in the economy and regulation processes in the cyber protection market.

2. **Systemic resilience:** "The ability of the state and its organizations to deal with cyber-attacks in a systemic manner in order to reduce accumulated damage to the economy before, during and after an event." This component is promoted by state processes of information-sharing and assistance to organizations that have been attacked.

3. **National defense:** "Managing a state campaign against serious threats, behind which are determined attackers with resources who pose a real risk to the security of the state."

National cyber security goals are focused on cyber security: building security capacity for prevention, dealing with cyber incidents when they occur, and managing overall efforts to weaken threats in the cyber field.

To realize these goals, five efforts are required:

1. Building cyber as a safe growth space: a government-wide effort that includes strengthening the protection of organizations in the economy, setting a high standard for the protection of government bodies, and implementing solutions, processes and infrastructure at the national level.

2. The establishment of the National Authority for Cyber Security and the promotion of complementary national preparedness: a central body with the sole purpose of cyber security.

3. Research, development and implementation of state defense capabilities and technologies.

4. Building national scientific-technological power in cyber as the comparative advantage of the State of Israel.

5. Partnership in international efforts to shape cyberspace.

The purposes of national cyber security efforts are broader than security-focused national security goals and correspond with the vision of a leading country in the cyber field. The existing national strategy has unresolved gaps between a broad vision of national leadership and the pursuit of cyber security.

Cyber security goals and efforts can be compared to the United States National Cyber Strategy of March 2023. The strategy's basic approach is to create a "path to [sustain] resilience in cyberspace." It emphasizes three principles: "rebalancing the responsibility for the protection of cyberspace" between users of the space and the giant companies that design and create the digital ecosystem; "rebuilding the incentives in a way that will prioritize long-term investments"; and basing the strategy on the achievements of current policy.

In order to realize the basic approach, five elements are defined, each of which is broken down into sub-elements:

1. Protecting critical infrastructures.
2. Identifying threat factors.
3. Letting market forces push for protection and resilience.
4. Investing in a more secure future.
5. Creating partnerships to achieve common goals.

The American strategy is thus focused on reducing inherent weaknesses and dealing with the threat potential: protection against cyber threats by closing loopholes in the existing lines of defense and information technologies; crafting a long-term vision; and proactively cooperating with others to pursue, disrupt and disable threat factors.

A similar approach focused on protection and reducing the threat can be identified in the goals of the work plan of the INCD for 2023. The first four goals (of seven) are: the establishment of a national cyber dome and within it a national SOC; realization of a sectoral and economic protection concept; directing the security activity according to national indicators; and providing a technological response to state cyber security. The following three objectives correspond with a focus on defense: advancing national interests through international partners; formulating state strategy and a regulatory concept; and integrating smart identification into the INCD.

It seems that the current American and Israeli approaches focus on defense aspects and are less preoccupied with promoting cyber security as a national economic and political multiplier, with the understanding that existing weaknesses require a focus on defense gaps and cyber incidents and threats. This is a realistic look at the cyber context and not one that tries to create, in the absence of strategic national documents, a broad strategic national context for the issue.

The issue for discussion: What should be the country's primary national goals in the field of cyber security? How to express and implement national cyber security goals? Should the focus on cyber security come at the expense of attention to projects in the fields of the national economy and security through cyber?

Recommendation: In defining national goals in the field of cyber security, Israel should put the needs of cyber security at the top. Only after answers to those needs have been found would it be correct to consider diverting residual resources to an issue that is not at the core of the defense.

Sub-issue 3a - The national cyber security circles

The State of Israel protects the central bodies in the economy against cyber threats to their supply chains through sectorial regulation, involving questionnaires and surveys, that requires them to examine their protection in a one-way customer-supplier channel. In this way, a wide range of large, medium-sized, and small business organizations that provide the central bodies in the economy with essential products and services are required to improve their conduct in a way that contributes to the overall level of protection of the state and the economy. This method has distinct advantages because it is based on effective means of regulatory compliance and business incentives, and it focuses the response on the work environment of the main sectors of the economy.

However, this approach contains several fundamental problems. The term "supply chain" was born of the point of view of the large organizations for which there are linear processes in which they gather inputs from a large number of sources (suppliers) in order to produce outputs that they sell to consumers.

But the world today is networked and non-linear. The "supply chain" image has to give way to the "network" concept. Almost all value factors in the economy find themselves on both the customer side and the supplier side. In such a world, the weakest link can bring down the entire network (which includes the supplier of the supplier of the supplier, or the customer who is also a supplier, etc.). In a small country like Israel, the national network is but a tiny part of a vast global network. This is particularly noticeable in the field of information technology. In 2017, for example, Ukrainian account management software damaged the functioning of, among others, the Danish shipping giant Maersk, the American shipping giant FedEx, and the American pharmaceutical manufacturer Merck.

Another problem with the "supply chain" approach is its bias toward promoting security through questionnaires and surveys. The big customer with many resources does not actually help the supplier improve its level of response to cyber security but spurs it on through "scores."

The solution to these gaps can come from a transition from the "supply chain" approach to a more comprehensive "supply network" approach. In this framework, government organizations and large business entities would strive to strengthen and protect the network around them, which would be based on regulation and guidance but also on practical steps to build effective protection in all circles.

How can such a network be built? Actual cyber security would be addressed in all its components within the framework of an integrated and synchronized concept at the national level. In this framework, for example, the following circles can be specified:

1. **Multinational corporations:** The most significant suppliers of the Israeli economy, especially in information technology, are the giants (e.g., Microsoft and Amazon in the cloud, Cisco and Intel in hardware, Salesforce, Swift in money transfers, Reuters in stock trading, and more). Along with organizational risk reduction and protection actions, a comprehensive national move is required to strengthen protection, with an emphasis on intellectual property and private information. In light of the size and distribution of these corporations, an effective move would require cooperation with them and with other governments, for example, the United States. Positive action of the national cyber echelon in this direction is expressed in goal 5.2 of the 2023 work plan: strengthening defense ties with multinational companies.

2. **Critical national infrastructures:** Bezeq, the internet and cellular providers, the electricity company, and others are another type of significant provider. Their security is largely managed, from a national point of view, under the INCD according to law, and in the past three years a leap forward was made in the security of the communication providers. It is required to add coordination between them and the rest of the economy (their customers) regarding cooperation in efforts to locate and handle cyber incidents in their

systems and improve the level of preparedness available to deal with a disruption of their services. Major steps in this direction have been made in recent years in the cooperation between the Ministry of Communications and the national cyber echelon. The prevention of cyber attacks that disable large communication companies is defined by the ministry as a target.

3. **Major Israeli information technology providers:** A number of large companies (for example, IT services and technology company Malam Team and trading platforms like FMR and Sivron) provide services on a wide scale. Some are even exclusive suppliers in their field. Unlike some of their customers, they are not subject to strict regulation in the field of cyber protection. A managed response at the national level for such bodies must be considered.

4. **Large supervised entities:** The large entities in the economy, some of which - especially the financial ones - are subject to regulation and supervision in the cyber field, should be the generators and accelerators of an increase in the overall level of security. For this purpose, Israel should consider expanding mandatory protection regulations to include, for example, all companies subject to the provisions of the Securities Authority.

5. **Medium-sized companies:** There are hundreds of companies in Israel that provide vital products and services to the economy (transportation and transport companies, large printing houses, information and trading applications, water corporations and more). Some are networked to the big bodies, affect the country's ability to function economically, and contain extensive intellectual property and private information. It is highly advisable to consider developing a broad national concept for these bodies that goes beyond current guidance and training efforts. Such a concept should include clear standardization, binding regulation, and a central body for advice, assistance and enforcement.

6. **Small businesses:** The tens of thousands of small businesses, a significant number of which are suppliers to large entities and some of which access highly sensitive information (e.g., law and accounting firms), also need an overall concept in the management of

a central body and decentralized execution that deploys an umbrella of protection over them and gives them access to cyber security services that they cannot maintain themselves.

7. **And finally, the entire public (the "customers")**: In a "supply network", as opposed to a "supply chain", the customers should be taken into account. A significant proportion of them are themselves suppliers of corporations and large companies, they have access to the information systems of those bodies, and they can to be a conduit of widespread cyber-attacks (e.g., DNS attacks). A response that raises the level of "cyber hygiene" of the general public by making information and means accessible is an inherent part of the vision of a "supply network."

In a discussion held on June 18, 2023 led by the INCD, Prime Minister Netanyahu ordered the minister, according to the summary announcement: "To prepare for the strengthening of the essential infrastructures and to advance the cyber security regulation of the entities that are responsible for them. In addition, the Prime Minister ordered a start to promoting a cyber protection law that will be based on international practice in the face of: 1. Regulation on critical infrastructure and 2. A standard for the entire economy."

The issue for discussion: Can the national cyber strategy take care of critical infrastructure and at the same time build a general standard for the entire economy, or should it deepen the segmentation of all the circles described and tailor a response - including national inputs mainly vis-à-vis international corporations - and in response to each of them?

Recommendation: As part of the strategic process, it would be correct to map the circles in which the governmental and business entities have difficulty providing an independent defensive response, and in which the state's activity can make a significant contribution in terms of closing the gaps and prioritizing the response to their solution. For example, the state level can set demands for international corporations and lead the process of building a reasonable program of "cyber hygiene" for the general public.

Issue 4 - The basic approach of the cyber security echelon

I do not wish to enter into the issue of legislation and regulation of the INCD. Rivers of ink have been spilled on this issue, especially around the failure of the debate surrounding the 2018 Cyber Security Act Memorandum and National Cyber Strategy. To my understanding, the main lesson from that event is the need to involve the largest organizations in the economy and the cyber expert community in the process. Since drafts of the new bill are already being circulated for reference among a limited group of experts and without wide transparency, it is not certain that this lesson has been implemented.

Out of all possible aspects of a basic approach to the national cyber security echelon, I believe there are two that require deep discussion beyond the legal system.

The first is the identity of the INCD as a body. It defines itself on its home page as “a state, operational and technological body entrusted with the protection of the national cyberspace and the promotion and establishment of Israel’s strength in the field.” The INCD can be any of the following models:

1. A security-operational organization that handles one of the threats to the State of Israel, similar to the IDF, the Mossad and the Shin Bet, which address other security threats.

2. A law enforcement organization that deals with crime in cyberspace, similar to the police and other enforcement bodies (the Authority for the Protection of Privacy, the Tax Authority, etc.).

3. A government regulation organization that guides government ministries on how to exercise their regulatory capabilities in their fields to ensure cyber protection in a manner similar to - but not fully compatible with - the National Security Headquarters.

4. A national organization that creates, guides, and enforces cyber protection regulation through cooperation and guidance as part of the 2016 amendment to the law regulating security in public bodies, being a certified officer for information security operations for fifty entities defined as critical state infrastructure that appear in the fifth

appendix to the law. According to the summary of the 2022 work year of the array, the list of included entities is updated every period by an inter-ministerial committee led by the head of the INCD. Guidance and control of these bodies are carried out on the basis of a manual with five steps and over 900 controls.

5. A national best practices and information body in the field of cyber protection similar to the National Road Safety Authority in its field.

There are other possible models, such as the Bank of Israel, which is a corporation whose main goal is to maintain price stability, but these are less relevant.

Following on from discussions on the national security circles, it can be said that for each of the circles and the challenges the INCD must face to realize its mission, a different mix of characteristics can be tailored. For example, critical national infrastructure already has an established formation as a national regulatory, guidance and enforcement organization. For government ministries and large entities in the economy that supervise, it is their right to function as a government headquarters and work organization. Small businesses and the public would work mainly as a body of national guidance and information.

The main problem with this approach is that it there may be contradictions between the various functions that would make it difficult for the parties in the various circles to cooperate. For example, if the formation takes on the powers of a security-operational organization or a law enforcement organization when dealing with a cyber incident in a civil organization, it may lose its ability to be a government regulatory body that guides the regulation, because the ability to act and direct enforcement may harm the relationship between the regulator and that civil organization.

In addition, while in cyber security assistance to the civilian economy, the INCD and the cyber security units in the various government ministries (comprising the 'national cyber security echelon') are unique and sometimes exclusive in their response, in the security, operational and enforcement aspects, Israel has bodies that are already engaged in handling the challenges. This should allow the national cyber security echelon to deal with the main gaps in the government ministries and the civilian economy and less on security-operational aspects.

The issue for discussion: First, what is the optimal mix of possible models of government organizations (security-operational, law enforcement, government regulation, national regulation, or a best practice body) that the national cyber security echelon can adopt in a way that would allow it to fulfill its duties in an optimal way at the various levels (defense, preparedness, incident response, enforcement and control, and active defense)?

The second aspect to be addressed is the subordination of the national cyber security echelon. This discussion is related to the identity of the INCD. The national cyber security echelon has grown over the years within the Prime Minister's Office and has been directly subordinated to the Prime Minister (with the exception of a period when it was allegedly subordinated to a minister working under the Prime Minister). This had substantial advantages that still exist. The ability to act independently, the backing of the Prime Minister, and the ex-territorial status of the government offices have all worked in favor of the system over the years.

However, it is not necessarily natural that dealing with national cyber security would be directly subordinated to the Prime Minister, and this may even increase the disadvantages over the advantages. The head of the INCD is not equal vis-à-vis the ministers, and therefore cannot guide the ministries without the full backing of the Prime Minister. The fact that a national cyber security law has yet to be enacted indicates the problem posed by direct subordination in the regulation process. The Prime Minister's attention to the INCD is very limited, which may make it difficult for it to promote initiatives that need his support. Being an independent echelon also distances it from areas of natural cooperation such as security, internal security and the promotion of national computing.

Other countries integrate cyber security within the overall system – either to a Ministry of Homeland Security or to a ministry that deals with technological innovation and national IT or to the Ministry of

Finance or Economy. Part of the process of maturing and normalizing Israel's handling of national cyber security, and managing the interfaces between the various organizations involved in it, could be the integration of the INCD into a proper government office.

The issue for discussion: Should Israel promote the integration of the INCD into a government office that will allocate it attention, interfaces and resources that it cannot receive from its independent position under the Prime Minister?

Recommendation: In decisions about the optimal mix of the characteristics of the INCD and its subordination, we must consider the most effective forms of influence government bodies have on what is done in government offices and the business sector. The INCD and the cyber security units in the government ministries (the 'national cyber security echelon') will focus on the protection of these bodies and not deal with national security, operational, or enforcement aspects that are handled by other organizations. In this framework, it appears that the combination between regulation and enforcement is the most effective.

Issue 4a - In the government sector

Over the years, the INCD has found it difficult to promote cyber security in the national government offices. The process of implementing cyber security and regulation processes and bodies in government ministries and national authorities has gone on for many years but has not yet reached the optimal point.

One indication of this is that in past years, references to cyber security aspects in the main work plans of the government ministry were sporadic to nonexistent. The document for 2023 showed a change that represents a step up in the attitude of government ministries to the issue. Apart from the INCD, the cyber security issue is mainly included in 10 out of 59 entities listed in the work plan, which constitute 18% of all government bodies – for some of which the issue of cyber security should not be a significant aspect of their activity. Significant ministries that have cyber security as part of their main work plans include the Ministry of Energy and Infrastructure, the Ministry of National Security, the Ministry of Innovation, Science and Technology, the National Digital Directorate, and the Ministry of Communications. It should be noted that the work plan of the Ministry of Intelligence (since then dismantled) includes goals for legislation and regulation in the cyber security field in collaboration with the INCD.

For some important government ministries, cyber security does not rise to a key section in the work plan - for example, the Ministry of Health, whose regulated organizations have suffered cyber-attacks in recent years, two of which developed into significant incidents. The director general of the ministry states in the introduction to the work plan that "at the global level there are new challenges such as a significant increase in cyber threats and attacks on health organizations in these areas," but the cyber issue does not appear as a goal in the work plan of the ministry. Other ministries that should have cyber security in their main work plans are the Ministry of Transportation, where a cyber-attack could have deadly implications; the Ministry of Interior in charge of the municipalities, where the state of cyber security - according to the state auditor's reports - is not good to say the least; and the Ministry of Education, which – together with the organizations subordinate to it – contains a great deal of sensitive personal identifiable information about children and teenagers.

Despite significant progress, the regulation of cyber security bodies and SOCs in government ministries, working in collaboration with the INCD, still does not always receive the attention and resources it requires.

The issue for discussion: How can cyber security be promoted in additional government ministries beyond those that have already made the leap (the Ministry of Energy and Infrastructure, the Ministry of Communications, etc.)? How can ministries’ cyber security receive attention and resources beyond what is currently provided (at the Ministry of Health, the Ministry of Transportation, the Ministry of the Interior, the Ministry of Education, and more)?

Recommendation: To increase the involvement of the INCD and push security activity in all government ministries and organizations, a central goal of the strategy should be to clearly prioritize cyber security in health, transportation, the interior (municipalities) and education ministries.

Issue 4b - In front of the business sector

The business sector still exhibits suspicion towards the INCD. Businesses find it difficult to see how they will profit by cooperating with it, while they can clearly see the costs in terms of attention and resources. The best way to involve these organizations may be through assistance in places where the state can do things the organizations are not strong enough to achieve. For example:

1. **National handling of the "supply chain":** As noted, a number of large international organizations and major Israeli companies are suppliers to hundreds of the largest organizations in Israel. Prominent examples are the clouds of AWS and Azure and the systems of Salesforce and SAP, which are found in almost every major company today. We can also mention Israeli companies like Hilan and MLM Salary, which handle salary calculations for almost all these companies. The state can identify the main horizontal suppliers and treat them like critical infrastructure in order to simplify corporate cyber security.

An example that clarifies this need is routers. During the Covid-19 period, when most of the economy switched to remote work, routers became a major risk factor for connecting to corporate networks. As mentioned, in the past two years the Ministry of Communications, in cooperation with the National Cyber Echelon, made a fundamental change in its policy on this issue.

2. **Regulation promotes positive change:** Regulation can be an excellent instrument for raising the level of cyber protection of the civilian sector. It obliges the organization to deal with issues that are not adequately addressed in the course of dealing with business considerations. However, requirements that are too specific, and that negatively affect the technological and business component and do

not leave discretion to the organizations, may alienate the companies, jeopardize the discourse, and compromise their cyber protection levels rather than improve it.

If the company's executives think the state is invading the core of its business considerations, and that regulators are operating out of a desire to utilize the capabilities of the company for their own needs, they will put in only the bare minimum investment required to pass the requirements. This problem is reflected in very detailed and intrusive reporting requirements on cyber incidents; anachronistic requirements that are not updated according to technological developments; and the ability to enforce and influence company decisions, which is perceived as draconian. See the previously mentioned extensive criticism of the 2018 Cyber Law affidavit.

Smart conduct by Israeli government agencies can promote cyber security and not impede it. Consider, for example, the banks, and the positive change they have undergone since the entry into force of Proper Banking Management Directive 361 in the field of cyber protection in 2015 and additional supplementary directives since then. These are worded in such a way that they leave the banks discretion over application and allow them to act according to their own individual characteristics. Compliance with regulations can also be accompanied by financial or reputational incentives. The US Department of Defense, for instance, awards annual certificates of excellence to companies that stand out in meeting their security requirements.

3. "A blanket of protection": The state has built-in advantages in terms of intelligence, early warning, knowledge and capabilities in the field of cyber and monitoring of national infrastructural bottlenecks. It can also respond with enforcement through legal and security-operational tools that can add an extra layer of protection outside of the organization. Many organizations would be happy to receive such help from the state, especially in response to extreme scenarios in which they are hit by a national state attacker – a situation that would require huge resources.

The creation of such a “blanket” requires that state bodies - with an emphasis on the INCD - commit to continuous action and to a level and quality of response that serves the needs of the organizations, especially in the face of very high-level attacks and the potential for unusual damage. In realizing the goal of “establishing a national cyber dome”, the INCD should focus on the ability to respond to these types of threats while building a bridge between the civilian economy and the security organizations. One of the complex challenges here is to mediate information - mainly alerts - from classified and highly sensitive intelligence sources to the civil organizations so they can provide an adapted response to both general and targeted threats.

4. **Addressing the manpower shortage:** Companies have a deep shortage of cyber security personnel. Good technologists often prefer to work at technology companies and start-ups due to the money and involvement in technological development, but most cyber security is done at large organizations and companies. A large company needs dozens of cyber people in various professions, from technological implementation to handling cyber security processes, and most companies in the Israeli economy have difficulty filling those ranks. The INCD can help through national programs for the recruitment and training of cyber defenders. The Ministry of Intelligence (dissolved since then) has set goals in this area that other ministries can adopt: "The Ministry of Intelligence is working to increase human capital skilled in cyber roles by increasing the employment of populations that are underrepresented in these positions (women, ultra-Orthodox, Arabs, residents of the periphery, discharged combat soldiers), as well as the need to promote exposure and experience programs in the field at a young age and continuing specialization programs at the high school age".

In recent years, the INCD has been dealing with the cyber security professions, including mandatory regulation of them. This process, which will be discussed below, is important first and foremost to promote the scope of employees with knowledge in the field of cyber security – not to create complex certification processes and disqualify good professionals who lack formal education.

5. **Working with cyber security services companies:** A significant force multiplier in the protection of the business sector is the companies that provide cyber security consulting services by offering surveys and penetration tests, implementing technological processes to investigate and forensically analyze cyber incidents, and providing fully paid cyber protection services (MSSP, CisoaaS). (For the sake of full disclosure, please note that this writer is connected to some of these companies). These companies should be perceived by the INCD as its long arm. The dialogue between the parties is sometimes suspicious, stemming from historical precedents in which the companies' knowledge was used without compensation, or large international consulting companies were preferred over local companies that are deeply familiar with the needs of the Israeli economy. Israel should examine the establishment of a mechanism involving, among other things, a forum of managers to ensure constant dialogue between the INCD and these companies.

The issue for discussion: How can the national cyber security strategy lead to strong and healthy cooperation with the business sector?

Recommendation: The solution of the horizontal difficulties - with an emphasis on the lack of skilled personnel in the field of cyber security - will be a central engine in the relationship between the INCD and the civilian economy.

Issue 5 - Efforts in the field of national cyber security

In this last part, I will refer in detail to several efforts in the field of national cyber security.

Cyber security training: In Israel there is an extensive industry in the universities, academic colleges and professional colleges dedicated to training for cyber professions.

The first issue here is scope. In the business sector there is a shortage of skilled personnel in cyber security. This is particularly important as ministries, government organizations and large companies transition to Nimbus, the government's public cloud computing project. Other issues are changes in the development processes of computer systems and the accelerated digitization and automation of security, which require more advanced professionalism among cyber security personnel. Training programs for the relevant cyber security professions should be expanded and accelerated while expanding cooperation with the major technology companies, academic institutions, and service and consulting companies.

The second issue is regulation. A significant part of the training is done on the basis of international standards. Graduates of cyber training programs must have sufficient knowledge to start working. For this purpose, a process of regulating the cyber professions has been promoted for several years. Technological progress affects the cyber professions, and individual adaptation is usually conducted through self-learning or through the organizations. In addition, the cyber occupation requires creative thinking and adaptation that is disconnected from information acquired in relatively rigid study programs. As a result, it is necessary to examine the mix between regulation of training and adherence to professional certification requirements before acceptance into the workplace and the need to preserve the flexibility, not covered by formal learning processes, that is needed to come up with new, creative solutions.

National encouragement of research and development (R&D) and cyber security industry development: Since the first incarnations of the INCD, the State of Israel has invested in promoting R&D and business entrepreneurship in the cyber security field. Encouraging R&D in cyber was defined as a goal in the 2011 cyber initiative. The national cyber strategy of 2017 describes an effort of "research, development and implementation of state security capabilities and technologies". The cyber entrepreneur Alon Arbats, in his book *The Best Defense* on the Israeli cyber industry, analyzes these efforts and concludes (p. 229): "It is difficult to overstate the value of the efforts of the State of Israel to create a favorable environment for the cyber industry, but it is important to be precise and see what from all these efforts really promotes the industry... cyber companies mainly need the freedom of private initiative, the quality manpower and capital that flows into the state to act together... the tax deductions and the low regulation [that] are many times more beneficial than the attempt to create another cyber center in Beer Sheva... growth depends not on what the state will do, but mainly on what it won't."

The INCD's work plan for 2023 is more modest than its predecessors in promoting R&D and defense products. It defines four areas in which to focus: protocol layer security, infrastructure to make cyber security services accessible, infrastructure to assess the level of resilience of the economy, and monitoring capability on a public cloud. This is a change from generally promoting the technology and industry of cyber security to providing a targeted response according to need. The State of Israel must break through in other critical areas such as quantum computing, artificial intelligence and alternative energy. All of these point to a need to restructure national supporting efforts in the field of cyber security R&D and industry.

International positioning and scope of cooperation: In summing up 2022, the INCD presented that it maintains an operational relationship with 33 countries and active partnerships in three multinational forums. The list of countries includes some of the leading cyber security powers in the world: the United States, Great Britain, Germany, Australia, and others (though it lacks leading countries in the field of defense such as France and the Netherlands). In the context of promoting Israel's foreign policy ("cyber diplomacy"), the list includes the countries of the Abraham Accords, the United Arab Emirates and Morocco, and key countries for Israeli foreign policy such as India, Japan, Greece, Cyprus, and others. However, looking at the list, it can be said that part of it represents the realization of opportunities for cooperation rather than a systematic plan that sets clear goals in terms of both cyber security needs and foreign policy goals.

Building partnerships is an essential supporting effort to the promotion of core cyber security such as operational security effort, technological cooperation, mutual learning and Israeli much needed influence on the formation of international norms in the cyber field. "Cyber diplomacy" is also a significant component in Israel's foreign policy toolbox. However, it is appropriate to direct the resources invested in this effort through a clear plan with rigid priorities and some flexibility for opportunities. Another issue that Israel must support, and that concerns many leading countries following the lessons of the war in Ukraine, is the building of a national capacity - in cooperation with the business sector - to provide a 'protective cyber dome' for the country if it enters into a state of war or cyber conflict with another country.

Learning from other countries versus tailoring a response to Israel: It is important to import the so-called best practices of cyber security from the world. We have a lot to learn in terms of systematicity and optimal management of the defense effort. At the same time, some of the requirements of the United States and Europe are more suitable to the national business culture of these countries - a culture of compliance and formal processes. This does not take into account the Israeli character, which contains both more room for creativity and diversity and a need for clear boundaries.

In Israel, a separation wall between routes - that is, cyber security based on technological limitations - is preferable to dividing lines that are drawn based on human action. Examples of the issue of compatibility with the Israeli character is the difference between the acceptance of the Cyber Security Proper Conduct of Banking Business Directive ('Nabat') 361 by the banks and the assimilation of the cyber defense doctrine for organizations version 1.0, which was distributed by the INCD in April 2018. While the NBT 361 is narrow in scope, it leaves quite a bit of discretion and flexibility regarding implementation up to the banks; detailed Excel listings of many hundreds of steps that organizations must take are much more difficult to digest and implement.

Noting the prime minister's meeting on June 18, 2023, the head of the INCD presented an international comparison according to which "Israel is in a gap in cyber regulation compared to advanced countries in the world, including Germany, Australia, the United Kingdom, the United States, and the European Union, [which legally regulate] the principles of risk management for essential organizations, the obligation to report cyber incidents, supervisory and enforcement powers for regulators, and … cyber security." There is no doubt that comparing the situation in Israel to the situation in the wider world is a useful tool when thinking about cyber security strategy, but to determine applicable principles, external models must be carefully filtered and adapted to unique Israeli characteristics.

Fixing the national compensation mechanism issue: Cyber insurance has expanded significantly over the past decade and is even in some cases a regulatory requirement. A major problem in the field of insurance coverage for cyber incidents around the world and in Israel is that there is a trend toward excluding state cyber-attacks in insurance coverage. As a result, organizations that appear to have been attacked by state entities are not entitled to compensation under the existing coverage. This issue is widely discussed in the insurance world. Since the burden of proof regarding the identity of the attacker is on the insurance companies, they drag national cyber security officials into the legal proceedings.

In Israel, the situation is more complex than it is elsewhere in the world because the business sector has been clearly and repeatedly attacked by Iran, Hezbollah, and Hamas, causing damage of various types as a result. The address for compensation for these damages is the property tax mechanism, but in the State of Israel there is no regulated process of attributing a cyber-attack to a state or terrorist entity and directing the victims to receive compensation from the state. It is obvious that this issue must be regulated, and the national cyber system should deal with it. It should also serve as a central enabler for the use of cyber insurance as a contributing component when responding to incidents.

The issues for discussion: To what extent and in what form should the national cyber array and national factors engage in the various cyber security efforts?

Recommendation: In the opinion of the author, the practice of training skilled personnel for cyber security for government ministries and the business sector should be greatly expanded and regulations in this field made more flexible. On the other hand, it is possible to limit and reduce national encouragement efforts in the fields of R&D and industry cyber security. It would be better to focus effort on the promotion of multinational collaboration in the field of cyber security according to strict

priorities with some flexibility for opportunities, including emergency aid to attacked countries. External cyber security norms should be adapted, provided those adaptations reflect the unique characteristics of Israel. It is also important to provide property tax compensation for cyber incidents caused by national rivalries and terrorist organizations.

Conclusion

This document was written, as noted, before the outbreak of the war, and its publication was delayed. In the framework of dealing with cyber threats during the war, very successful national efforts are evident, especially in terms of the cooperation between the INCD and governmental units and the civilian cyber security ecosystem of Israel.

In the writer's opinion, the security efforts during the war sharpen the discussion of the connecti o n of cyber security to national security strategy and national security doctrine, both of which collapsed on October 7.

These efforts also suggest ways to focus Israel's national cyber security goals and define the national cyber security "circles", and add new layers and experiences to the discussion about the place of national cyber security apparatuses in the government sector and vis-à-vis the civilian sector.

On the other hand, the cyber threat that materialized since October 2023 corresponds to a war scenario and is not necessarily the required threat profile for peacetime, which we hope will be more prolonged.

Recent BESA Center Publications

Mideast Security and Policy Studies

No. 178 Israel Versus Anyone: A Military Net Assessment of the Middle East, *Kenneth S. Brower*, August 2020

No. 179 The EU and Israel as Genuine Strategic Partners, *Florin Pasatoiu and Christian Nitoiu*, August 2020

No. 180 The Israel-UAE Peace: A Preliminary Assessment, *Editor: Efraim Karsh*, September 2020

No. 181 The American Public and Israel in the Twenty-First Century, *Eytan Gilboa,* October 2020

No. 182 Iran Behind the Scenes During the Second Israel-Lebanon War, *Raphael Ofek and Pesach Malovany,* November 2020 (English and Hebrew)

No. 183 The Pentagon's UAP Task Force, *Franc Milburn,* November 2020

No. 184 The Second Nagorno-Karabakh War: A Milestone in Military Affairs, *Uzi Rubin,* December 2020 (English and Hebrew)

No. 185 Iran's Killing Machine: Political Assassinations by the Islamic Republic, Ardavan Khoshnood, December 2020

No. 186 The Battle for the Soul of Islam, *James M. Dorsey,* January 2021

No. 187 The Caspian Sea as Battleground*, James M. Dorsey,* February 2021

No. 188 The Abraham Accords: Contrasting Reflections, *Shmuel Trigano*, March 2021

No. 189 American Development of UAP Technology: A Fait Accompli?, *Franc Milburn*, March 2021

No. 190 Should Israel Cooperate with the ICC? *Anne Herzberg*, March 2021

No. 191 The Logic Behind the JCPOA—Then and Now, *Oded Brosh*, May 2021 (English and Hebrew)

No. 192 Middle East Futures: Defiance and Dissent, *James M. Dorsey*, June 2021

No. 193 ASMLA: An Empirical Exploration of an Ethno-Nationalist Terrorist Organization, *Arvin Khoshnood*, June 2021

No. 194 The Laundromat: Hezbollah's Money-Laundering and Drug-Trafficking Networks in Latin America, *Emanuele Ottolenghi*, July 2021

No. 195 The 2021 Gaza War: The Air Campaign*, Ehud Eilam*, July 2021 (Hebrew only)

No. 196 The Radicalized Israeli Arabs, *Efraim Karsh*, August 2021

No. 197 A New Palestinian Authority NGO Decree Might Halt US Aid to the West Bank and Gaza, *Dore Feith*, August 2021

No. 198 Iran's Nuclear Program: Where Is It Going? *Raphael Ofek*, September 2021

No. 199 The Nagorno-Karabakh Conflict: Roots and Consequences, *Galit Truman Zinman*, September 2021

No. 200 Russia's War Against Ukraine - Impacts on Israeli Nuclear Doctrine and Strategy, *Louis René Beres*, April 2023

No. 201 The War in Ukraine: 16 Perspectives, 9 Key Insights, *Eado Hecht, Shai Shabtai (Eds.)*, August 2023

No. 202 The Oslo Disaster 30 Years On, *Efraim Karsh*, September 2023

No. 203 National Cyber Strategy: Issues for Discussion, *Shai Shabtai* , January/June 2024

No. 204 The War of October 7 – and the One to Follow, *Eran Ortal*, February 2024

No. 205 Israel Needs a Sustainable Strategy, *Eran Ortal*, April 2024

No. 206 War With Iran: Israel's Legal Obligation to Prevent Iranian Nuclear Weapons, *Louis René Beres*, June 2024

besacenter.org