Dmitry (Dima) Adamsky

The Israeli Odyssey toward its National Cyber Security Strategy

Governments around the world are transforming themselves to meet the challenges of the cyber era. Israel is at the tip of the spear: its model brings tangible results, its best practices serve as an example to be emulated, and by distributing knowledge it has positioned itself as a source of learning to other nations. The United States, a global cyber leader in resources, science, and technology, has been highly impressed by the progress of the Israeli cyber community, learning its path, listening to its cyber leaders, and adhering to their vision.[1] The centrality of the Israeli case to exploring the cyber aspect of international relations is thus unquestionable.

Until recently, however, scholars predominantly focused on the military component of the Israeli case, overlooking a major issue—the comprehensive Israeli vision of the cyber phenomenon and its policy logic in the cyber domain. Recent works examining archetypical cyber security models have started to explore this issue.[2] Their important contributions notwithstanding, they have focused mainly on the organizational and historical aspects, partially due to the fact that the conceptual aspect of the Israeli approach has become publicly available only recently, with the forthcoming publication of the first Israeli National Cyber Security Strategy.[3] This article aims to fill this void. Based on previously unavailable primary sources and interviews with Israeli officials, it presents the unique strategy that Israel has recently designed for the cyber domain.

This article argues that the Israeli cyber odyssey, and the national cyber strategy that constitutes its peak thus far, stands out in terms of its comprehensiveness,

Dmitry (Dima) Adamsky is Associate Professor in the Lauder School of Government, Diplomacy and Strategy at the IDC Herzliya, Israel.

The Washington Quarterly • 40:2 pp. 113–127
https://doi.org/10.1080/0163660X.2017.1328928

vision, and successful political fate. By scrutinizing the Israeli cyber innovation, this article seeks to offer insights that are applicable beyond the Israeli case for theoreticians and practitioners dealing with cyber aspects of international security policy. The article consists of three parts: The first outlines the historical context to the formulation of the Israeli national cyber security strategy; the second highlights the main components of the strategy; and the third discusses the intellectual subtext of the Israeli cyber innovation. The conclusion discusses the ramifications for international affairs.

Israeli Cyber Odyssey: the Context

The context—the intellectual organizational history and the main events that motived Israel's cyber decisions—is important to understand the essence of the 2017 Israeli national cyber security strategy. A bevy of cyber security activities in the mid-1990s preceded the current national-level effort. As the Israeli government dealt with Internet connectivity, early e-Government, and web services, it started to grasp the essence of the information technology (IT) revolution and recognize its potentials. Experienced defense experts introduced civilian leaders to the potential risks and opportunities of the IT domain. They bridged the knowledge gap about IT security concerns as well as solutions—for the leadership and for government branches.[4]

Mentored by the defense establishment, in 1997 civilian leaders established the Tehila Unit, which was charged with coordinating state infrastructure for the Internet Era and increasing productivity, efficiency, and security throughout the government. Until 2002, however, the overall response to the cyberspace risks and opportunities was sporadic. Most government agencies pursued their cyber security efforts parochially—in a disjointed, localized, and incoherent manner—hardly coordinating with Tehila. Israel's emphasis on science and technology led to impressive capabilities and awareness, but IT security efficiency across the government lagged. Gradually, the government realized that cyber security was not just a technical matter but a huge policy issue that demanded cultural-organizational transformation.[5]

Israeli experts mention two major events motivating national IT awareness and decisions.

When asked if there were, in addition to the leadership's growing IT awareness, any specific episodes that motived national-level decisions, senior Israeli cyber experts mention two major events, totally unrelated to IT: Prime Minister (PM) Yitzhak Rabin's assassination in 1995 and the 9/11

attacks. According to them, the failure to warn of and prevent Rabin's assassination was a colossal intelligence blunder. Shaped by the traumatic experience of the 1973 war surprise, to better prepare for future out-of-the-blue attacks, such as the PM's assassination, Israeli intelligence experts started to think outside the box to imagine the unthinkable. These efforts to expect the unexpected garnered the insight that intelligence blunders in the IT era, linked with critical infrastructure, might result in colossal national catastrophes. The major intelligence surprise in September 2001 further strengthened this insight. Together with the leadership's IT awareness, it motivated internalization of the potential cyber risks and accelerated the tempo of the government's cyber odyssey.[6]

The first landmark of the national-level effort was the Critical Infrastructure Protection (CIP) arrangement. In 2002, the government tasked the National Security Council to outline strategies for the emerging risks. The work resulted in Special Resolution B/84 on protecting computerized systems in the State of Israel. This resolution established centralized Critical Infrastructure Protection and defined the goals and means of Israeli cyber security, becoming one of the first national cyber security policies in the world. Considering further policy steps, the government realized that leaving cyber security to market forces or to the IDF was impossible. Driven by ethical and legal considerations, it authorized the National Information Security Authority of the Israel Internal Security Service (Shabak) to protect vital computerized systems of selected public and private civilian organizations. Although the arrangement is still intact, it was greeted with reluctance by the private sector, which assumed that it might hamper innovation and economic growth. Since then, Israeli cyber security policy has been seeking a modus vivendi between the government and private corporations, trying to balance market efficiency, science and technology, basic freedoms, and privacy with IT security.[7]

The discontent with the state of cyber security resulted in a political will to develop national cyber security policy, looking beyond IT-security in the critical infrastructure and defense sectors. Not driven by any specific event,[8] but by the basic recognition of the growing impact of cyberspace, in 2011 Prime Minister Netanyahu set up the National Cyber Initiative taskforce to pursue a comprehensive approach to cyber security, exploring potential macroeconomic and strategic benefits for Israel. The taskforce headed by Prof. Gen. (ret.) Isaac Ben-Israel was the watershed and fundamental enabler toward the next milestone. This independent multi-stakeholder taskforce produced a report that laid the de facto foundation for the Israeli national cyber policy for the years to come. The policy recommendations covered the spheres of education, R&D, security, economic development, and international cooperation. The main practical recommendation was to establish a new governmental cyber security organ to realize and coordinate these policy efforts.[9]

Following these recommendations, the second milestone was the establishment of the Israel National Cyber Bureau (INCB), subordinated to the Prime Minister's Office, as a sign of importance and source of bureaucratic power. Codified in 2011 by Government Resolution 3611 'Advancing the national capacity in cyberspace,' the INCB was charged with fostering the national cyber policy. This effort was aimed at enabling Israel's overall defense and maintaining its status as a global cyber-power, while also achieving economic, technological, and diplomatic benefits. The Bureau's mandate was to formulate a comprehensive and formal cyber strategy, which should replace all previous narrow resolutions, to articulate and lead national cyber policy; advise the government on cyber matters; advance R&D in academia, the educational system, and industry; develop cyber-technology as an economic growth engine; and leverage cyber security for international cooperation. Supported by financial capacity, and capitalizing on the immediate proximity to the Prime Minister, the INCB quickly established itself as the conductor of the Israeli cyber orchestra and has been influencing short- and long-term policy in various realms of defense, academia, and industrial sectors.[10]

Three years of internal staff work by the INCB resulted, among its other projects, in finalizing the cyber posture through two legislative initiatives. This was the third milestone toward the strategy. In a way, prepared by the INCB, the initiatives already encapsulated major principles and contents of the future strategy. Although Israeli national cyber policy was driven by the assumption that the public-private nexus would be a central component in defending cyberspace, until 2015 Israel's approach was seen as incomplete and inadequate since it was almost exclusively focused on high-quality defense of critical infrastructures and security bodies. Almost all of the principles of the required national response had not been implemented, let alone as part of an integrative whole.[11]

In 2015, the Government passed resolutions Nos. 2443 and 2444 that established a national cyber security regulatory mechanism and national regulator-operator in this field. Both resolutions aimed at mitigating the complex, non-technological, moral, legal, and organizational tensions between the state's security needs and basic freedoms, and at facilitating a comprehensive cyber security policy. This codified national response, emphasizing the civilian (including the governmental) sector, established the necessary cooperation, mobilized national capabilities, and coordinated relevant efforts. The end result was the establishment of the National Cyber Security Authority in 2015 and publication of the comprehensive National Cyber Security Strategy, which encapsulated insights from several classified white papers published internally since 2012. Thus, the 2017 National Cyber Security Strategy is the culmination of an almost decade-long odyssey, providing a comprehensive policy framework.[12]

National Cyber Security Strategy: the Essentials

The 2017 strategy regulates the state's conduct in the cyber security realm along three interrelated vectors. The first chapter, "Concept of Operations," outlines the actual set of activities aimed at cyber defense; the second chapter, "Capacity Building," outlines the set of R&D, industrial, and educational undertakings aimed at producing capabilities enabling the concept of operations; the third chapter, "Structure," outlines the mandate and configuration of the Israeli National Cyber Directorate (INCD) responsible for overseeing the first two endeavors.

The Concept of Operations (CONOP)

The Israeli concept of operations consists of a three-layer framework.

In a nutshell, the Israeli CONOP consists of the "Three Layer Framework"—*robustness*, *resilience*, and *defense*.[13] The first layer, "*robustness*," refers to "the capacity of the organization to perform without failure, by repelling and containing threats in the national cyber domain" under a wide range of conditions.[14] To illustrate the first layer, Israeli cyber experts offer parallels from the world of medicine. They compare "robustness" with the ability of the human body's immune system to routinely withstand the negative influences of the natural environment.[15] Likewise, organizations should systematically maintain cyber immunity by adopting specific technological-bureaucratic procedures, including educational and training activities, which increase awareness and reduce the probability of a successful attack or of substantial damage. State actions to enhance each and every organization's cyber hygiene, and its overall maintenance, are expected to ensure national-level cyber robustness.[16] Although the first layer is seen as generic cyber prowess, unrelated to any specific act, it ensures optimal conditions for the "event-driven" activities under the auspices of the second layer—*resilience*.

"*Resilience*," according to the strategy, stands for the "capacity to handle attacks in order to regain overall normal functioning"of the organization.[17] In contrast to the first layer, which is essentially a generic cyber vaccination, this layer is an event-driven effort; it refers to an organization's ability to recover from threats, which have materialized and stricken it, and the state's ability to prevent the potential cumulative national effect of these strikes. Separately or jointly with the affected organization, the state's involvement grows exponentially in this layer, and includes detection of the threat, confining the expansion of its infiltration, mitigating its effects, and denying its reoccurrence. The government conducts these activities through its national cyber events response team (IL-CERT).[18] Along the lines of the medical analogy, this layer can be considered

as parallel to the healthcare system's ability to handle specific injuries, where vaccination and hygiene are insufficient and direct medical involvement is needed.[19]

Finally, the "*defense*" layer of the concept of operations stands for the national efforts, of both offensive and defensive nature, vis-à-vis high-end cyber threats. Here, in an effort to manage a mega-incident, countermeasures should be tailored to the specific attacker and to the overall strategic logic of an attack's ends, means, and ways. This demands a national-level effort beyond defensive cyber activities and involves proactive offensive moves—cybernetic and kinetic—by organs of law enforcement and national security against state and non-state initiators of the attack.[20] While "*robustness*" is purely the responsibility of the organization, with the state playing an incentivizing and enabling role, "*resilience*" is a joint venture of the organization and the state, "*defense*" is within the state's exclusive authority.[21]

Although Israeli cyber experts dub the third layer "defense," it is much more offensive in nature, focusing on the specific attacker and the means of attack, whereas the first two layers ("*robustness*" and "*resilience*") are purely defensive in nature. Moreover, these first two layers charge the batteries of cyber deterrence by denial, while the third layer, despite its given name but due to its offensive nature, enables deterrence by punishment.

Capacity Building

Summed up briefly, the "*capacity building*" chapter encapsulates several endeavors aimed at fostering the national cyber ecosystem. These efforts include supporting and stimulating state-owned industry as well as private commercial R&D in the leading cyber fields, fundamental and applicative academic research, and cultivating scientific-technological human capital throughout all stages of education, from elementary to high school. Last but not least, capacity building refers to state-sponsored R&D of prospective cyber dual-use national-level technologies, an endeavor, in the words of Israeli experts, along the lines of the U.S. DARPA (Defense Advanced Research Projects Agency) best practices.[22] The chapter reflects concrete projects implemented by Israeli cyber policymakers during the last years in all the above fields to ensure that Israel secures its position as one of the world's leading cyber powers.[23]

To develop high-quality human capital, the Israeli government, through the INCB, has been allocating hundreds of millions of dollars for the consolidation of supportive academic research and in R&D grants to companies and universities.[24] To market cyber products globally, the Israel Export Institute established a unit that promotes cyber technology field exports through Israel's commercial attaches worldwide.[25] During the Davos World Economic Forum, the Israeli PM arranged an exclusive meeting with global cyber industry leaders to further

leverage Israel's position in the field and to encourage their investment in and cooperation with the Israeli cyber industry.[26] Unsurprisingly, more than 30 multinational companies have identified Israel as the optimal location for the development of cutting-edge capabilities and knowledge in the cyber security field and are engaged in extensive activity there. In the field of security for Industrial Control Systems and security for the Internet of Things, Israeli companies, according to Dr. Eviatar Matania, the INCD head, and Tal Goldstein, the INCD Chief Strategist, "are at the forefront of global technology, and to a considerable extent are even ahead of the market."[27]

Israel has been allocating hundreds of millions of dollars to develop human capital.

Absolute and relative numbers speak for themselves. In global private investment in cyber security firms, "Israel is second only to the United States, with half a billion dollars flowing to the sector annually."[28] In 2015, acquisitions of Israeli cyber companies totaled over $1 billion, while investments totaled over $250 million.[29] Exports of the Israeli companies generate $3.5–4 billion per year—about 5 percent of the global cyber security market (and more than 7 percent of the global cyber security products market).[30] To ensure the continued prosperity of the Israeli cyber industry, Israel took a calculated risk and further liberalized, in the summer of 2016, its cyber-related exports and licensing policy.[31]

IBM, Lockheed Martin, Deutsche Telecom, PayPal, EMC and JVP have already become part of the Israeli national endeavor to create a cyber ecosystem in the Beer-Sheva Cyber Park.[32] Envisioned as the cyber capital of Israel and as one of the cyber centers of the world,[33] the Beer-Sheva cyber city has been concentrating talents from the military, academia, and business, including the deployment of the IL-CERT operating from there, to create a vibrant entrepreneurship environment and foster the next rounds of innovation. No other country, not even the United States, "is so purposefully integrating its private, scholarly, government, military and intelligence cyber expertise" to ensure cross-pollination.[34] An Israeli replica of Silicon Valley, this "Desert Valley" is aimed at enabling the Israeli cyber sector to turn the place into an economic powerhouse, regionally and globally.[35] Before and especially after the national cyber regulation, governmental leadership in the cyber security sector is seen as an engine for the economy and as an activity that more closely links the public and private sectors to their mutual benefit, economically and for security.[36] Thus, the "capacity building" part of the strategy somewhat codifies the existing reality.

The Structure of the Cyber Directorate

The strategy document also outlines the "*structure*" of the main Israeli cyber organ and the logic of its configuration.[37] Israeli experts assumed that none of the institutions within the Israeli national security community dealing with various aspects of the cyber realm was relevant to dealing with the national-level task. According to them, putting the main cyber organ within one of the existing sectors of internal or external security would be an erroneous and piecemeal decision. The alternative solution makes it possible to avoid the bureaucratic-organizational imprint that any sectarian stakeholder might leave on the cyber politics. Consequently, the strategy institutionalizes a supra-ministerial organ exclusively cut off for this task, and reporting directly to the Prime Minister. The *Israeli National Cyber Directorate* (INCD) is the highest national authority for strategic cyber policy planning, for the regulation of its operational execution across the government, and for building cyber capabilities for the short, medium, and long term. Until now, only three organs in Israel had the same exclusive subordination status: Mossad, Shabak, and the Israeli Atomic Energy Committee.[38]

The Directorate consists of two arms. The first, the National Cyber Bureau, is responsible for the overall strategic policy planning in the realm of capacity building, and the second, the National Cyber Security Authority, is responsible for the national-level implementation and regulation of the three layers of CONOP, including CERT-IL of the critical infrastructures. As such, the Directorate unites under one roof organs leading the three vectors of the CONOP—robustness, resilience, and defense. The Directorate is also responsible for leading and facilitating international cooperation and formulating the legal framework for cyber activities domestically and internationally. During peacetime routine, the INCD is responsible for the comprehensive management of the national defense campaign, while other military and security agencies wage any offensive undertakings. At times of emergency, the IDF becomes the national-level integrator of the offensive and defensive campaigns.[39]

Holistic Israeli Cyber Mentality: the Subtext

Although comparative study establishing the distinctiveness of the Israeli strategy in relation to cyber doctrines worldwide is beyond the scope of this article, outlining the conceptual guidelines, which the Israeli cyber leadership adopted for its strategy, may be valuable. Highlighting self-reflections of the Israeli cyber experts on their approach and depicting their mindset may offer useful food for thought and a frame of reference for cyber policy practitioners dealing with similar tasks elsewhere.

The INCD seniors commenting on the approach that guided them while designing the strategy's essentials qualified it as holistic, comprehensive, and long-term.[40] To ensure these characteristics in budget allocations, state level R&D, and human capital development, they sought to design the widest possible national cyber ecosystem. They also ensured that the structure of the new national-level regulator-operator (recall that the NCB and NSA both regulate and operate cyber affairs on the national level) is designed in a way that enables it to overview, guide, and sustain this ecosystem by embracing all of its dimensions.[41] The cyber architecture designed in the strategy distinguishes itself from the majority of cyber management models worldwide by establishing a new organ with a unique concept of operation, the CONOP, beyond existing institutions.[42]

The holistic mindset of the INCD experts emanated from, among other things, the distinct vision of the cyber realm, which demanded parting ways with the traditional strategic planning process. Typically, governments in Israel and worldwide, when dealing with national and internal (criminal) security affairs, have focused on the potential challenger and then tried to deter, prevent, or defend an attack from him. Consequently, they allocated jurisdiction according to the identity of the perpetrator, qualifying an assault either as an act of war by a state, or as a crime, international or domestic, by a group or individual. Since identifying the perpetrator in the cyber realm is challenging, post-factum attribution difficult, and differences between the perpetrators often blurred, Israeli experts saw such a traditional division of jurisdictions as irrelevant.[43]

Instead, they sought to pursue a perpetrator-indifferent approach that encompasses the entire range of cyber challenges and creates a national-level holistic remedy. Consequently, Israeli strategy builds immunity vis-à-vis fundamental but generic threats—existing and prospective, known and unknown. It assumes that protection of the specific asset is more important than dealing with the perpetrator, and focuses on the types of possible attacks and on the specific assets whose protection is vital, regardless of the attacker.[44] The Israeli approach focuses on critical national targets that should be protected against a diapason of threats—what the head of the INCD dubs "Cyber Iron Dome,"[45] alluding to the Israeli "terminal" missile defense system aimed at hermetically protecting the hinterland from mid-range ballistic threats, no matter where they originated.

The distinct vision of the cyber realm parted ways with the traditional strategic planning process.

Also, the INCD seniors sought to formulate a strategy that preserves its long-term relevance with no need for frequent updates. To ensure the strategy's non-sensitivity to inevitable technological innovations and to immunize it against

political uncertainty, the INCD distilled several principles that are likely to remain intact, irrespective of prospective future developments.[46] Three insights turned into basic assumptions on which the strategy rests. First, regardless of the IT operating system, the organization would be the basic target of any cyber security challenge. Since organizations own the networks, the organization is therefore a basic frame of reference in the Israeli approach and an elementary unit of analysis in the strategy rather than individual, group, or state.[47] Second, the cyber-security threats are borderless. State cyber borders are nonexistent because any state "borders" the rest, regardless of the geographical distances. In contrast to classical warfare, where the military buffered between the enemy and the rear, in the cyber realm organizations themselves become the first line of defense. Cyber guards along state borders that filtrate the harm are not an option. Consequently, the third assumption that only organizations themselves could address the problem by building up their cyber self-defense, which the national strategy should enable them to do effectively.[48]

Why Cyber is Different for Israel

This article has highlighted the historical context and the intellectual subtext of the Israeli national cyber security strategy, and analyzed its essence—the multi-layered defense CONOP protecting the national cyber ecosystem; the capacity building that enables it; and the organizational configuration that executes it. Israel's cyber odyssey, culminating in the national strategy, is a major departure from tradition since Israel never had an official strategy driving its security policy. In the 1950s, the first Prime Minister, David Ben-Gurion, formulated the principles of the security concept, which then drove Israeli strategic practice for decades.[49] Several efforts to institutionalize this unofficial concept, update it, and turn it into a formal strategy repeatedly failed.[50] The political fate of the cyber endeavor is strikingly different. The recommendations of the task force headed by Isaac Ben-Israel, together with the national strategy produced by the INCD under Eviatar Matania, can be paralleled to Ben-Gurion's national security concept. The cyber strategy is the first successful Israeli effort to produce a coherent national security white paper that de jure drives long-term policy formulation and de facto regulates its operational execution.

The cyber strategy is Israel's first successful effort to produce a coherent national security white paper.

Scholars offer several explanations for the Israeli cyber success. Geopolitically, science and technology have traditionally been equalizers of Israel's quantitative

inferiority. This was especially true during the IT-RMA era, out of which the cyber age matured.[51] As part of this approach and faced with sophisticated security demands, organizationally the State of Israel has been persistently (since roughly the 1960s-70s) pinpointing and training the best and the brightest of its scientific-technological youth toward, and during, compulsory military service. Enjoying access to the national reservoir of talent, this perpetual machine has been intact for several generations.

As a result, annually a cadre of technologically educated and experienced youth leaves the military and joins the professional and academic workforce, enhancing the national cyber ecosystem. Israeli universities and high schools, well supported by the government, ensure a solid scientific-academic foundation for providing this human capital. Geographical-institutional proximity, an informal communication style, a non-hierarchal business atmosphere, and networking culture have ensured cross-pollination and made Israel a natural hub for cyber cooperation, competition, and innovation.[52] It seems like Israeli leaders skillfully produced a balance between the deep perception of the cyber phenomenon and exploiting the Israeli culture of improvisation, ingenuity, and entrepreneurship.[53] One of the main sources of the INCD's success was an ability to capitalize on the graduates of the most prestigious military-technological higher education programs of the IDF, in particular of the Talpiot.[54]

As a former graduate and then head of the program, Matania nominated several of its alumnae to the leading INCD positions, naturally involving them in strategy formulation. Their main competitive advantage was their unique academic training, which combined a most rigorous technological education with a relatively solid acquaintance with the strategic studies discipline, the mix allowing a broad national security perspective on cyber affairs. Such a cadre enabled the INCD to overcome a major staffing problem characteristic of cyber policy organizations worldwide, where experts with a cyber background have difficulty embracing holistic strategic perspectives, while "strategists-generalists" are illiterate regarding the deep mechanics of the cyber realm.

Finally, the Israeli PM has been closely associated with the national cyber leap forward. Viewing himself as a figure with a unique role in Jewish history, Netanyahu sees himself as the protector of Israel, repelling existential geopolitical threats, and as someone who revolutionized the Israeli market, ensuring economic prosperity and growth. Regardless of the accuracy of these self-attributions, he envisions cyber as one of the mega trends, enabling him to promote his visionary goals—a perception that results in prioritization of the cyber agenda and unparalleled enhancement of the INCD directly subordinated to him. The combination of visionary political and professional leadership, according to U.S. experts, accounts, among other things, for Israel's leading position in cyber-security affairs.[55]

What are the ramifications of the Israeli cyber innovation in the realm of international politics? First, Israel is, probably, a world pioneer in inaugurating cyber diplomacy as a soft power instrument. Netanyahu has been repeatedly highlighting "cyber hopes" no less than "cyber risks," arguing not only for solutions to Israeli defense but also for public goods for the wellbeing of mankind. He sees cyber as one of the best trade commodities worldwide, perceives IT as a tool for bringing people closer, and believes that Israel's neighbors can benefit from its cyber security solutions. During the last decade, one of the main drivers that prompted the BRICS (Brazil, Russia, India, China, and South Africa), as well as several Arab and African states, to approach Israel has been their desire to seize the opportunities in the cyber realm. Israel has benefited from this economic-scientific cooperation, but also translated it into a more favorable position of these countries toward Israel in various international forums.[56] Thus, the cyber charm offensive has become one of the main endeavors in the Israeli struggle for international attractiveness.

Israel is probably a world pioneer in inaugurating cyber diplomacy as a soft power instrument.

Second, if Israel succeeds in utilizing cyber to enhance international ties and as a bridge for cooperation and mutual prosperity, it might become a platform for regional normalization. In the summer of 2016, Israel and the United States signed a cyber defense declaration calling for real-time operational connectivity through respective Computer Emergency Response Teams (CERTs).[57] Israel is considering similar agreements with others. If these materialize, they may serve as a platform for expanding cooperation and reaching out to countries that traditionally Israel had less developed ties with, in Latin America and Asia, and further forging ties with Europe and Middle Eastern states. Utilized in conjunction with other moves, it could enhance regional interdependence, which in turn may increase the degree of strategic stability.

Last is the issue of international cyber regulation. Israel's leaders' perception of their state's international role in the cyber domain somewhat corresponds with Eisenhower's "Atoms for Peace" initiative. Israel is steadily promoting its version of "Cyber for Peace" of sorts, emphasizing opportunities no less than dangers, despite the threats and limitations involved in international cyber cooperation,[58] and despite alternative views within the Israeli strategic community.[59] The "Atoms for Peace" speech became a precursor to the international regulator (International Atomic Energy Agency or IAEA) and regulation (Non-Proliferation Treaty or NPT) in the nuclear realm. Similarly, growing Israeli global cyber diplomatic activism and the country's self-perception as a leading world cyber power might further contribute to the global zeitgeist bringing the

world cyber community, of state and non-state actors, closer to joint regulation in the cyber realm.[60]

Notes

1. U.S. Department of Homeland Security, "Remarks by Deputy Secretary Alejandro Mayorkas at the 6th Annual International Cyber Security Conference," June 22, 2016, https://www.dhs.gov/news/2016/06/22/remarks-deputy-secretary-alejandro-mayorkas-6th-annual-international-cybersecurity. Admiral Michael S. Rogers, Commander, United States Cyber Command / Director, National Security Agency – Testimony before the Senate Committee on Armed Services, May 9, 2017, (min 46), https://www.armed-services.senate.gov/hearings/17-05-09-united-states-cyber-command.
2. For example, see: Narmeen Shafgat and Ashraf Masood, "Comparative Analysis of Various National Cyber Security Strategies," *International Journal of Computer Science and Information Security* 14, no. 1, (January 2016); Daniel Benoliel, "Towards a Cybersecurity Policy Model: Israel National Cyber Bureau Case Study," *North Carolina Journal of Law and Technology* 16, no. 3, (March 2015); Lior Tabansky, "CyberDefense Policy of Israel: Emerging Threats and Responses," *Chaire de Cyberdefense and Cybersecurite*, January 2013; Gil Baram, "The Effect of Cyberwar Technologies on Force Build Up: The Israeli Case," *Military and Strategic Affairs* 5, no. 1, (May 2013).
3. The staff work on the final version of the Israeli national security cyber conception is currently at the final stages. Even if the bureaucratic-organizational dynamic continues for a while, and whatever form the final product receives (i.e. published whitepaper or internal concept), the essence, the contents, and the main pillars of the strategy have already became available from the INCD senior officials. For example see: Dr. Eviatar Matania, Keynote at 7th Annual Billington CyberSecurity Summit, September 13, 2016 available on YouTube at: https://www.youtube.com/watch?v=GMf8HMC0QeQ. On the structural aspect of the concept see: Eviatar Matania, Lior Yoffe, and Tal Goldstein, "Structuring the National Cyber Defence: in Evolution Towards a Central Cyber Authority," *Journal of Cyber Policy* 2, no.1 (2017), pp.16-25.
4. Lior Tabansky and Isaac Ben-Israel, "Cybersecurity in Israel," *Springer Briefs in Cyber Security*, (New York, 2015), chapter 4.
5. Lior Tabansky and Isaac Ben-Israel, *Cyber Security in Israel*, (New York, 2015), chapter 4.
6. Interview with Erez Kreiner, former head of the Shabak's National Information Security Authority, Central Israel, February 2017; Interview with Eviatar Matania, head of the Israeli National Cyber Directorate (INCD), Central Israel, February 2017.
7. Prime Minister's Office, "Background for the establishment of the National Cyber Bureau," http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/Background.aspx; Tabansky and Ben-Israel, *Cyber Security in Israel,* chapter 5.
8. Interview with the INCD seniors, Central Israel, February 2017.
9. Ram Levi (ed.), *National Cyber Initiative: Special Report to the PM* (State of Israel, Ministry of Science and Technology, May 2011) (Hebrew); Tabansky and Ben-Israel, *Cyber Security in Israel,* chapter 6.
10. Interviews with Eviatar Matania, Tal Goldstein (the INCD Chief Strategist), and Lior Yoffe (the INCD Head of Defense Planning), Central Israel, 2015–2017; Tabansky and Ben-Israel, *Cyber Security in Israel,* chapter 7.

11. *Background for the Government Resolutions Regarding Advancing the National Preparedness for Cyber Security and Advancing National Regulation and Governmental Leadership in Cyber Security*, February 15, 2015, State of Israel Prime Minister's Office National Cyber Bureau (Unclassified). Tabansky and Ben-Israel, *Cyber Security in Israel*, chapter 8; Author interviews with Eviatar Matania, Tal Goldstein, and Lior Yoffe.
12. *Background for the Government Resolutions Regarding Advancing the National Preparedness for Cyber Security and Advancing National Regulation and Governmental Leadership in Cyber Security*, February 15, 2015, State of Israel Prime Minister's Office National Cyber Bureau (Unclassified). Tabansky and Ben-Israel, *Cyber Security in Israel*, chapter 8; Interviews with Eviatar Matania, Tal Goldstein, and Lior Yoffe.
13. For a detailed analysis of this part of the strategy, see: Eviatar Matania, Lior Yoffe, Michael Mashkautsan, "Three Layer Framework for a Comprehensive National Cyber Security Strategy," *Georgetown Journal of International Affairs* 17, no. 3, (Fall/Winter 2016), pp. 77-84.
14. *Ibid*., pp. 4-5.
15. Interviews with Eviatar Matania, Tal Goldstein, and Lior Yoffe; Benjamin Netanyahu, "Remarks at the Cyber-Tech Conference," Tel Aviv, January 26, 2016.
16. An Israeli government resolution from 2015 obliges every ministry to allocate 8 percent of its budget to cyber security needs. Eviatar Matanya, "Opening Speech at CyberTech 2015," Tel Aviv, March 24, 2015.
17. Interviews with Tal Goldstein (the INCD Chief Strategist), and Lior Yoffe (the INCD Head of Defense Planning), Central Israel, 2015–2017.
18. Eviatar Matania, Lior Yoffe, Michael Mashkautsan, "Three Layer Framework for a Comprehensive National Cyber Security Strategy," pp. 6-7.
19. Benjamin Netanyahu, January 26, 2016; Interviews with Tal Goldstein and Lior Yoffe.
20. Eviatar Matania, Lior Yoffe, Michael Mashkautsan, "Three Layer Framework for a Comprehensive National Cyber Security Strategy," pp. 6-7.
21. Eviatar Matania, Lior Yoffe, Michael Mashkautsan, "Three Layer Framework for a Comprehensive National Cyber Security Strategy," pp. 8-9. The overall responsibility for coordination at the time of emergency moves to the military side of the strategic community (see the "Structure" section below).
22. The INCD experts often use the DARPA analogy as a frame of reference to illustrate their intentions. Interviews with the INCD senior officials, Central Israel, 2015–2017.
23. Interviews with Tal Goldstein and Lior Yoffe; Netanyahu in Cyber Tech Conference, 2016.
24. Eviatar Matania and Tal Goldstein, "Growing in Numbers, Sophistication and Strength," *Israel Defense*, January 2016, pp. 7-8.
25. Matania and Goldstein, "Growing in Numbers."
26. Managing directors and senior figures in the global cyber industry, including from Sony, Hitachi, Lenovo, Intel, IBM and Hewlett Packard, participated. Israeli Ministry of Foreign Affairs Press Office, "PM Netanyahu meets with global cyber industry leaders in Davos," January 21, 2016, http://mfa.gov.il/MFA/PressRoom/2016/Pages/PM-Netanyahu-meeting-with-global-cyber-industry-leaders-21-Jan-2016.aspx.
27. Matania and Goldstein, "Growing in Numbers."
28. Ellen Nakashima and William Booth, "Cyber-city rises from the Desert in Israel," *The Washington Post*, May 15, 2016., https://www.washingtonpost.com/world/national-security/how-israel-is-turning-part-of-the-negev-desert-into-a-cyber-city/2016/05/14/f44ea8e4-0d58-11e6-bfa1-4efa856caf2a_story.html?utm_term=.b7e68a505180.
29. Eviatar Matania, "Opening Speech at CyberTech 2015," Tel Aviv, March 24, 2015.

30. Matania and Goldstein, "Growing in Numbers."
31. Barbara Opall-Rome, "Israel Liberalizes Cyber Export Policy," *Defense News*, June 21, 2016, http://www.defensenews.com/story/defense/2016/06/20/israel-liberalizes-cyber-export-policy/86144694/; PM Netanyahu in Cyber Tech Conference, Tel-Aviv, 2016.
32. Matania, "Opening Speech at CyberTech 2015."
33. Netanyahu in Cyber Tech Conference, 2014.
34. Nakashima and Booth, "Cyber-city rises from the Desert in Israel."
35. PM Netanyahu in Cyber Tech Conference, 2016.
36. *Background for the Government Resolutions Regarding Advancing the National Preparedness for Cyber Security and Advancing National Regulation and Governmental Leadership in Cyber Security*, p. 5.
37. See: Matania, Yoffe, and Goldstein, "Structuring the National Cyber Defence."
38. Eviatar Matania, "Remarks at the IDF National Security College," Central Israel, Summers 2015 and 2016; Benyamin Netanyahu in Cyber Tech Conference, Tel Aviv, 2016.
39. Interviews with Tal Goldstein and Lior Yoffe.
40. Interview with Eviatar Matania and Tal Goldstein, Central Israel, February 2017.
41. Interviews with Eviatar Matania, Tal Goldstein and Lior Yoffe.
42. Eviatar Matania, Lior Yoffe, and Tal Goldstein, "Structuring the National Cyber Defense: In Evolution Towards a Central Cyber Authority," *Chatham House* (forthcoming, 2017).
43. Interviews with Tal Goldstein and Lior Yoffe.
44. Interviews with Eviatar Matania, Tal Goldstein and Lior Yoffe.
45. Matania, "Remarks at the IDF National Security College."
46. *Ibid*.
47. *Background for the Government Resolutions*.
48. Interviews with the INCD experts, 2015–2017, Central Israel.
49. Isaac Ben-Israel, *Tfisat Ha Bitahon Shel Israel* (Tel Aviv: Universita Meshuderet, 2014).
50. Charles Freilich, *Zion's Dilemmas: How Israel Makes National Security Policy* (New York: Columbia UP, 2014); Dima Adamsky, *The Culture of Military Innovation* (Pale Alto: Stanford UP, 2010).
51. Tabansky and Ben-Israel, *Cyber Security in Israel*, chapters 1 and 2.
52. Netanyahu in Cyber Tech Conference, 2014; Matania and Goldstein, **"Growing in Numbers";** Matania and Goldstein, interviews; Tabansky and Ben-Israel, *Cyber Security in Israel*, chapter 3.
53. Dan Senor and Saul Singer, *Start Up Nation* (New York: Twelve, 2011); Dima Adamsky, *The Culture of Military Innovation* (Pale Alto: Stanford UP, 2010)**.**
54. Jason Gewirtz, *Israel's Edge: the Story of the IDF's Most Elite Unit – Talpiot* (Jerusalem: Gefen Publishing House, 2016).
55. U.S. Department of Homeland Security, "Remarks by Deputy Secretary Alejandro Mayorkas."
56. Netanyahu, Interview in Davos (2016). Netanyahu in Cyber Tech Conferences, 2014, 2016.
57. Opall-Rome, "US-IS Sign Cyber Defense Declaration."
58. Netanyahu, Interview in Davos (2016); Netanyahu in Cyber Tech Conference, 2016.
59. The Head of Israeli Military Intelligence argued that new media and cyber capabilities have so far had mostly a destructive rather than constructive strategic influence, regionally and internationally. Head of Israeli Military Intelligence, General Hertzi Halevi, Speech at the 2016 Herzliya Conference, June 16, 2016.
60. Netanyahu in Cyber Tech Conference, 2014.