Photo: Shutterstock

The Elusive Presence of Technology in Israel's Strategic Security Thinking

Eviatar Matania, Oren Podhorzer, and Nir Daniel

Tel Aviv University

Israel's scientific and technological posture and its military-technological advantage are a result of strategy and force concentration over years. The continuance and maintenance of this advantage depend on correct strategy and decisions. Technological capability and technological edge are commonly assessed by budget allocations or by academic research ranking, industrial R&D, and investments in human capital. This essay addresses the subject from a different perspective, and examines the place of technology as reflected in Israel's official security strategies published over the past two decades. This perspective reveals to what degree the role of technology in future-oriented national strategic planning is understood. Analyzing three central Israeli security strategies, the essay looks at the place of technology in a normative understanding of how complete technological strategies should be written; compares these strategies to one another in the context of the technology component; and then compares them to the national security strategies of the US and UK. Israel's scientific-technological standing and its military-technological edge are an outgrowth of many years of strategic effort. Nonetheless, while the strategies explicitly discuss the technological edge as an objective (ends), they lack a comprehensive analysis of how to achieve it (ways) and what tools are needed to build technological strength (means). The article concludes with a discussion of the implications of the lapse in these strategies.

Keywords: technology and security, national strategy, national security, technological strategy, Israel's security doctrine

Introduction

The overarching view in Israel among decision makers, academics, and the lay public regarding technology in general and military technology in particular vis-à-vis national security and military security are: Science and technology are vital infrastructure for a developed nation and a central component of Israel's national security in the broadest sense; technology is considered a decisive element for every military's efforts to gain the upper hand on the battlefield; because Israel suffers from severe quantitative asymmetry against its enemies, technology is particularly essential to achieve the military superiority necessary for its survival; Israel has had a decided technological edge over its environment for many years; it has an advanced technological posture globally with leading science and technology industries, and a particularly significant posture in military technology based on excellent independent R&D.

Indeed, over the years the understanding that technological superiority and outstanding scientific-technological human capital are significant elements in maintaining the edge over rivals has increased and become a fundamental component of Israel's security strategy, in the broad sense and in the military-security sense (Ben-Israel, 2013; Ben-Israel et al., 2020, pp. 8-21; Matania, 2022; Finkel & Friedman, 2016; Eilam, 2009, pp. 497-508; Amidror, 2020).

Creating and maintaining a leading technological posture requires steady, long-term investments in academic scientific infrastructure, technology systems infrastructure, and human capital, which constitute the foundation on which technological force buildup is possible. Such investments bear fruit only many years later, sometimes only after a decade or more. For example, investments in scientific and technological human capital in Israel prior to the establishment of the state were what enabled independent R&D in the decades after its establishment. Investments in human capital in the first decades of the state's existence were the foundation on which it was possible to achieve military and technological superiority from the 1990s onward, and were one of the components that allowed Israel to become a hub of technological innovation (Matania, 2022).

Research Question and Methodological Approach

The question addressed in this article is: To what extent do Israel's current strategic planners understand the importance of science and technology as a strategic component of the state's national security and a key component of its regional military advantage, and to what extent do they deliberately cultivate these fields based on a strategic leadership vision. There are several ways to address this question. Two common ways to answer it are through measurement and analysis of technology budgets, and indices that measure the level and breadth of R&D. The first focuses on analyzing various budgets allocated to technology, from general R&D budgets (such as for the Planning and Budgeting Committee and the Innovation Authority) to the allocation in the defense budget for technological capacity building, as well as R&D budgets in the business sector, in comparison to previous years and to other countries, in relative or absolute terms. The advantage of this method is that there is typically a high degree of correspondence between R&D budgets and the breadth of R&D conducted, but the method is imperfect given that it does not measure quality and is insensitive to focused effort strategies or redundancies.

A second common method is comparative measurements of R&D bodies in Israel, such as universities, the tech industry, and security R&D, in relation to other countries around the world, on a per capita or absolute basis. Regarding the civilian sector there are many statistics and rankings that show that Israeli academia is in a solid position in science and the Israeli tech industry is in a good position in a number of areas, such as cyber or data science. In the security realm such measurement is more complex, but possible. The advantages of this method are the ease of comparison to the rest of the world, and the use of relatively objective measurements. Its disadvantages are that it measures the current reality, which relies on investments and efforts made decades ago, and that rankings sometimes miss the real story of R&D and may mislead those considering where to go from here.

This paper takes a third approach, which does not rely on budgets or statistics, but rather on the state's strategic declarative level, in order to examine how and to what extent the issue of technology figures in Israel's core strategic plans at the level of national security and the level of military defense. There are obvious drawbacks to this method: first, statements are not the same as actions ("easier said than done"). Some countries profess extensively but in practice do little, due to inability by various sectors to implement plans, or because budgets are not delivered, notwithstanding promises and planning. Second, this method relies on the thought and writing of security strategies and their authors, yet in the State of Israel there is a noticeable lack of written, authorized national strategic plans; Israel is stronger in practice than in theory.

At the same time, this method has several advantages. First, when a certain subject appears in a clear, orderly manner in national security doctrine, this indicates awareness and commitment among the top echelon of strategic decision makers, who will therefore presumably allocate the resources necessary to address it over time. It is eminently possible that this commitment will remain consistent from one governing coalition to the next. Furthermore, clear and committed statements about strategic directions diffuses downward to the professional and operational ranks in a unified manner. They serve as a compass for long-term action, because these formal statements have practical implications for the depth of comprehension in setting strategic plans and targets, determining strategic priorities, writing long-term and five-year plans, allocating resources, and developing suitable human resources. Likewise, an extremely important advantage is that the contents of strategies determine future outcomes, which is at the heart of this study, rather than merely take a still photo of the present reality, which relies on what others built decades ago.

Furthermore, examining national strategies reveals the motivation and vision they put forward to the nation as a whole and those who work in the field; these are often much more significant than funding. Israel is a good example of a country that in its early decades lacked funding but made a concerted national effort to allocate scarce resources to science and technology, based on the clear vision and strategy of its leadership. It thus successfully built itself as a leader in security technologies and later in overall tech, in a manner disproportionate to its size. Budgets and rankings did not measure or show this clearly for decades.

Thus despite the inherent shortcomings, this method is chosen for the purpose of understanding the place of technology in the state's strategic agenda. Though incomplete, it constitutes an important avenue to a comprehensive view of the question. To this end, it studies Israel's security strategies written in latter decades and examines whether they officially reflect the drive for technological advancement and the incorporation of the technological element as a fundamental pillar in Israel's national security strategy for the future; how technology is reflected in Israel's strategic security thinking; and whether the official expression of this thinking matches its importance.

This article analyzes the discussion of technology in three central security strategy documents written in Israel in the past twenty years, which represent the place of technology in Israeli security thinking. The first is a document recommending a national security strategy prepared by the Meridor Commission in 2006 and presented to the Olmert government. Although it was not officially ratified, it is considered one of the seminal documents in the national security field in the past two decades. The analysis of this article relies on the reassessment in 2018 of the original version (Meridor & Eldadi, 2019). The second is the *IDF Strategy* in its unclassified version, which was published in an updated version in 2018 (*IDF Strategy*, 2018), and reflects technological-security thinking on the military-security level. This IDF publication, first released in 2015, aimed to explain its strategy from the comprehensive viewpoint necessary for its national security concept. The third is the Israeli cyber security strategy (*Israel Cyber Security Strategy*, 2017) which, although it relates to a particular issue within the field of national security, discusses it at both the level of overall national security and at the specific defensive level.

In other words: The first strategy examined is at the level of national security (narrowly defined, not in the broad sense that includes social and economic aspects, but rather classic security alone); the second strategy is one level below, i.e., defense in the broadest sense; and the third is the cyber security strategy, which is comparable to the previous two (i.e., it aims at two levels) but focuses only on the specific issue of cyber. We thus gain a wide view of national strategies from two directions (overall and focused) at two levels (national security and military defense), developed by three different bodies (an appointed committee, IDF General Staff, and a governmental body). To the best of our knowledge, no other national or quasi-national strategies have been issued in recent decades regarding security or national security, except for a confidential document of former Prime Minister Netanyahu that cannot be accessed. This article thus covers all existing written and unclassified strategies in this field.

The methodology for analyzing and comparing these strategies is an analysis of ends, ways, and means. As defined by General Lykke, strategy can be described as the link between these three components (Cancian, 2017). This theory posits that balancing these three components is necessary for creating a successful strategy; conversely, when they are not balanced the strategy will not be realized successfully (Yarger, 2008).

Based on this methodology, the strategies are analyzed in three different ways. First is an analysis of the technological elements in these strategies in relation to what is an expected connection between ends, ways, and means. This gives us an initial *normative* view of what is present and what is lacking from these strategies regarding technology, in comparison to what we would expect from each, given its scope and focus, and in comparison to the extent to which it addresses other, non-technological issues. Second is a *comparison between the three strategies*, not of their contents (which discuss different subjects at different levels), but in terms of their discussion of technology, in accordance with the subject matter and scale of each document. In other words, we compare the way they discuss technology, and the comprehensiveness and scope of this discussion. Third, the Israeli strategic discussion of technology is compared to that of two counterparts, namely, security strategies in Western countries—the United States and the United Kingdom. This comparison allows a *comparative politics* view of two security and technology powers, which serve as a basis of comparison for the role of technology in national strategy.

Nonetheless, a few caveats are in order regarding this methodology. First, the American and British strategies used as a basis for comparison are at the highest level of national strategy, and are thus primarily suitable for comparison to the Meridor Committee report on Israel's national security doctrine. At the same time, however, they give an excellent perspective on how to relate comprehensively to technology, which is also relevant for the lower levels of IDF strategy and Israel's national cyber security strategy. In addition, the US and UK documents were approved formally on a national level by state leaders. In contrast, the Israeli documents were not formally approved by the government and thus do not necessarily reflect the security concepts of the leadership—either when they were written or today. This caveat is particularly important regarding the National Security Doctrine (the Meridor Committee): the team that wrote it was established at the request of Prime Minister Ariel Sharon and its conclusions were submitted to Prime Minister Ehud Olmert for approval by the government, but it was never approved or given formal authorization. This caveat is also partially relevant for the *IDF Strategy* and the *Israel Cyber Security Strategy*. These are products of the IDF and the National Cyber Directorate, respectively, which were approved by their directors when they were published, but which were never adopted by the government.[1] Furthermore, the discussion of technology in each document is different, in accordance with the documents' respective strategy levels and objectives. *The IDF Strategy*, for example, which reflects awareness of a national security strategy, does so from the military strategic viewpoint of the IDF Chief of Staff, which combines a concept of IDF operations with organizational decisions about the IDF.

Nonetheless, it appears that the method chosen in this essay for analysis of Israeli strategy for maintaining a technological edge in the future—a central and vital element in national security—is particularly strong. The analysis encompasses three inherently different documents written by different authors in different organizations, and the analysis from three different directions based on a comparative doctrinal basis allows an objective overview of Israel's strategic approach to the place and role of technology in national security.

Despite the centrality and importance of the technological edge, and the degree to which the Israeli strategic security establishment and decision makers rely on this edge for both national security and military defense, it is not addressed in a comprehensive manner. Plainly put, this discussion is far from what would be expected from a leading tech power such as Israel.

The article's primary claim is that despite the centrality and importance of the technological edge, and the degree to which the Israeli strategic security establishment and decision makers rely on this edge for both national security and military defense, it is not discussed and addressed in a sufficiently comprehensive manner. Plainly put, this discussion is far from what would be expected from a leading tech power such as Israel. In other words, there is a disparity between stating the importance of technology and building a comprehensive technology strategy for maintaining Israel's technological edge. This work examines the three security strategies in order to confirm this claim and show that it is especially relevant for national security doctrine and IDF strategy; it is partly relevant for cyber security strategy. This disparity is emphasized by the comparison to the foreign strategies (US and Britain) that discuss this issue comprehensively. It then addresses the reasons for this disparity and the implications therein.

Part I: Israel's National Security Strategies and the Role of Technology

Israel's Security Doctrine: The Meridor Committee a Decade Later

General

Israel's National Security Doctrine: The Report of the Committee on the Formulation of the National Security Doctrine (Meridor Committee), Ten Years Later (Meridor & Eldadi, 2019) examines the concluding report of the committee headed by Dan Meridor on formulating Israeli's security doctrine, which was submitted in April 2006 to then-Prime Minister Ehud Olmert and then-Minister of Defense Shaul Mofaz. The report aimed to sketch insights and basic principles for the national security doctrine of Israel, while focusing on a narrow definition of the concept of security. It included almost no discussion of the elements of national security in the wider sense, except for briefly touching on central national issues that interface with the security realm, such as the idea of "the people's army" or the portion of the security budget in the overall state budget. The document enjoyed a wide consensus regarding both the need for the document and its contents. Though never formally approved by the government, some of the report's recommendations were adopted in practice, such as the addition of a "defensiveness leg" to Israel's accepted security triangle and its incorporation in IDF strategy.

The Role of Technology

The centrality of technology in the security doctrine is already clear from the core principles, with two out of nine principles (principles 4 and 8) directly discussing the qualitative technological edge: "Israel's [security] power will be based primarily on independent national strength, which relies on maintaining its qualitative edge"; and "promoting the qualitative edge requires that relative advantages be exploited on the national level. To that end, human capital should be nurtured, technological opportunities should be utilized, and organizational ability should be developed" (Meridor & Eldadi, 2019, pp. 22-23).

The former principle cited implies that the lion's share of Israeli security strength derives from its technological and human quality edge, and the latter explains in general terms how to further develop this qualitative edge. The aspiration to maintain and strengthen this qualitative edge relies on two key efforts, which complement one another. The first is the cultivation of human infrastructure and creation of a technology base. The foundation of the human and technology base comprises the quality of human resources both in the IDF and in industry, the groundwork of advanced security R&D infrastructure, security industries that develop and manufacture advanced armaments, and international cooperation. The second effort is translating this foundation into military power, which relies on the development and acquisition of advanced armaments, the acquisition of systemic capabilities based on operational concepts, the cultivation of quality manpower for command, operation, and maintenance of weapons, and the creation of an organizational infrastructure in the fields of management, knowledge, and information.

The document then offers recommendations for building military capacities (pp. 35-36), contending that the approach to military force buildup must balance force buildup for countering specific threats, i.e., a responsive approach—"force buildup is a kind of 'response' given to an anticipated 'threat,'" as described by Isaac Ben-Israel (1997), with a generic approach of versatile solutions that enable relatively quick building of military capabilities. This approach resembles that of Yoram Hamo (2016), which relates to force buildup as a two-sided war, whereas what is required is to maintain the existing comparative advantage over regular armies in the region. The document also included concrete recommendations for directions of technological development, including advancing unmanned capabilities (such as UAVs), advancing precision weapons, developing the space field, developing anti-rocket defensive capabilities, and more.

The document also expands on the need to regulate a national decision making structure regarding the qualitative edge from an interdisciplinary and inter-organizational perspective. It recommends designating a single security body as responsible for setting priorities, making central decisions, and creating a regular binding coordination mechanism among R&D systems that must, in light of resource limitations, be focused and relevant, work in a timely fashion, and have the potential to translate ideas into effective solutions that generate a substantial advantage on the battlefield (pp. 44-45).

Analysis

Technology is clearly accorded a central place in the overall national security doctrine. In accordance with the classification of the components of strategy, the technological edge is a central means to create Israeli security strength, which is a way to achieve national ends. There is a partial description of how to maintain the qualitative technological edge (ways), and an understanding that in order to maintain it there is a need to cultivate human capital that can build technological infrastructure, which is a basis for building advanced military capabilities. However, there is a noticeable lack of discussion of how human capital should be cultivated, and little discussion of the concrete ways in which the qualitative edge should be maintained (for example, the scope of investment required in security R&D, the connection between academia and human capital, and more). This absence is especially noticeable in comparison to the discussion of other issues in the document that are addressed extensively as to "what" and "how," such as the challenge of terror.

In practice, military defense for the State of Israel relies on US security aid and cooperation to maintain its technological military superiority.

The IDF Strategy Document

General

The IDF Strategy is a comprehensive conceptual document that was initially published for the general public in 2015 and updated in 2018, with the aim of constituting a theoretical and practical framework for all IDF military activity (*IDF Strategy*, 2018). This was the first time that the IDF published such a document, which aimed to explain its strategy from the broad viewpoint necessary for the IDF's national security approach. It thus became a seminal document that explains the concepts, emphases, focus, and conclusions of the professional ranks of the military. The document describes the IDF's strategy as a means for achieving national interests, and relies on the foundations of military thinking and action. It proceeds from the general to the specific: it starts from the strategic framework—national aims, strategic environment, threatening actors and their characteristics, and principles of the national security concept and their link to the aims and mission of the IDF (ends). It then discusses principles and approaches to the use of force, the concept of command and control, and principles of force buildup in the short and long terms (ways), and the capabilities needed by the IDF (means). The strategy in the document relies on four pillars, in accordance with the recommendations of the report on Israel's security doctrine discussed above—deterrence, warning, defensiveness, and clear and decisive victory over the enemy, while implementing them in a defensive security strategy and an offensive operational military concept (p. 9).

The Role of Technology

Technology in the *IDF Strategy* appears in a number of aspects. Regarding Israel's strategic environment, the document shows that the rapid pace of technological development, the enhancement of technological capabilities for military uses, and the information and cyber revolution fundamentally influence the strategic environment, thereby influencing national security and the IDF in particular (pp. 10-11). With respect to the military aspect of the IDF's opponents ("the red side"), the document presents a significant threat to the IDF resulting from the trend of increasingly wide distribution of technologically advanced weapons and enemy buildup with offensive and intelligence components that aim to disrupt IDF capabilities and operational superiority in all dimensions of combat (pp. 12-13). As part of the IDF strategy, it is necessary to prevent, disrupt, and negate the technological enhancement of the state's enemies, during both times of routine and emergency, in order to maintain the gap and the technological edge via prevention and influence, which includes active steps to prevent this enhancement during periods of calm (pp. 15-16). *The IDF Strategy* relates to intelligence and particularly to technological intelligence as a foundation for understanding the enemy, its capabilities, and its intentions, as part of the process and the learning competition between the State of Israel and its enemies. This is a central component in adapting solutions and technological operational capabilities to negate the enemy's capabilities on the one hand, and maintain the qualitative comparative edge on the other hand (pp. 10, 17, 20).

The central purpose of the technology aspect in the *IDF Strategy* is to maintain the qualitative comparative edge and allow overall deterrence vis-à-vis enemies in different arenas. According to the document, Israel's qualitative comparative edge must be maintained while continually studying the strategic and operational environment and following the enhancements of other militaries in the Middle East as part of a competition of learning, in order to ensure preservation of the qualitative edge (pp. 21, 26).

With respect to the use of force, the document obligates the IDF to conduct force buildup processes to maintain and strengthen Israel's military status and maintain its qualitative comparative edge and military superiority in all dimensions (land, air, sea, intelligence, and cyber), while constantly meeting the challenges of the rapid, frequent pace of technological change and economic challenges. In particular, the document specifies the need for advanced technology adapted to operational needs and for appropriate means and experienced manpower. It places technological manpower in the Group A priority list, alongside combat soldiers as a high-quality force for combat missions on the battlefield. It likewise describes the principles of force buildup, including flexibility and versatility, networking, interconnectivity, critical mass, lethality, freedom of action, and strengthened learning processes (pp. 25-30).

In contrast with force application, technological force buildup is not presented in the *IDF Strategy* through a clear strategy and methodology that defines ends, ways to achieve them, and necessary means, and the reciprocal relations among them. The document defines the ends of force buildup as maintaining and strengthening Israel's military status while allowing the use of force according to the responsive approach, but not the core capabilities required for technological force buildup. Beyond the general principles of force buildup, the document does not deal with ways and means for techno-operational force buildup, for example, investment in R&D, development and cultivation of human capital, cooperation between industry, the Ministry of Defense, and academia, make-or-buy decisions, and more. This gap reflects inadequate strategic thinking between operational approaches to the use of force and processes of force buildup from a holistic view, and this impairs the completeness of the overall strategic outlook presented.

Analysis

The IDF Strategy reflects a theoretical and practical framework for all military activity as part of Israel's national security concept. It discusses implementing the strategy, with an emphasis on the use of force, the challenges of combat, and the definition of operational needs, with the response relying inter alia on advanced technology.

However, regarding the need to maintain the qualitative comparative edge and technological force buildup, the *IDF Strategy* lacks a discussion of the processes of technological force buildup (ways), construction of a strategic process to this end, including implementation, supportive organization, required resource allocation, prioritization, make-or-buy definitions, security-technology cooperation, and especially a strategic conceptual connection between the needs and operational objectives (ends), the ways to achieve them, and the resources and technologies required to do so (means). It is therefore clear that in contrast with other aspects in the strategy, the technological discussion is insufficient and does not depict the central role that technology in all its aspects (use of force, force buildup, organization, and resources) must play.

An additional central component lacking in the technology context is that of national and international cooperation as a key component in realizing the strategy, and especially strategic-security cooperation with the United States. In practice, military defense for the State of Israel relies on US security aid and cooperation to maintain its technological military superiority, especially for equipping itself with advanced weaponry (such as the Adir F-35 planes) that Israel has neither the desire nor the financial capability to develop on its own (Rounds, 2019, pp. 36-37—cancellation of the Lavi project). This subject is also not discussed in the *Strategy*.

Israel Cyber Security Strategy

General

The National Cyber Directorate document (2017) describes the mission of the national cyber security strategy "to regulate all national efforts in the field of cyber defense, to create a 'common language' among all those working in this field, and to ensure a stable and long-term solution" (p. 8).[2] The document comprises three sections. First is a description of the operational concept for cyber defense, which consists of three layers of defense. Second is a description of the manner of implementing the strategy based on three overarching efforts: building cyber as a secure, thriving space by implementing the three layers of defense; establishing an operational arm of the Cyber Directorate to lead efforts to defend the Israeli economy from attack; and ensuring research, development, and implementation of defensive state technologies. The third section is a description of scientific-technological force buildup for cyber and strengthening Israeli's comparative edge in this field, along with the importance of international partnerships for shaping the cyber space.

The Role of Technology

Technology is discussed in the three main sections of the strategy. In the first section, which discusses the way (ways) to fulfill the aim of defense, the technologies required for each layer (means) are described as an essential part of the defense layer. In the second part of the document (pp. 37-38), technology is described in an especially prominent manner as part of the third effort—research, development, and implementation of advanced defensive state technologies, as well as a dedicated state R&D unit (the Cyber Technology Unit), which is entrusted with the technological force buildup for national cyber defense and mandated to provide solutions to operational needs of the Cyber Security Authority. In other words, according to the strategy proposed in the document, an overarching R&D effort of advanced national defense technologies is necessary, as one of the three principal components of defense—evidence of the central role technology commands in this strategy. The final section describes the supporting efforts for consolidating national cyber capabilities, one of which is scientific-technological force buildup in cyber (pp. 42-46). The document discusses the matter of force buildup and human capital extensively, and addresses two additional areas: incorporating academia in the cyber ecosystem, along with industry and human capital; and enhancing the quantity and quality of human capital, starting from a young age (junior high school and high school students), as a basis for future human capital.

Analysis

Technology appears in this document as both a structured means for achieving the ways of defense, in accordance with the model of the three layers (the first section of the document); as ways of achieving stable, long-term defense in itself by building a dedicated unit for technologies and R&D (the second section); and as an end in itself in building the complete cyber ecosystem in Israel (the third section). The strategy presented in this document is considered especially complete and comprehensive in the field of Israeli strategy. It makes clear connections between ends, ways and means, and technology is interwoven in all its aspects and sections in a comprehensive manner (Adamsky, 2017). A fundamental part of this strategy is maintaining Israel's technological edge in this field.

The Role of Technology in the Different Strategies: A Comparative Analysis

In the three strategies examined, technology appears as an essential component for Israel's strength in each of the fields with which the strategies engage. In Israel's *Security Doctrine*, the technological qualitative edge appears in two fundamental principles underlying the doctrine. In the *IDF Strategy*, the technology facet appears early in the document vis-à-vis the comparative edge as a principle for strategic strengthening of the State of Israel (and later, the comparative edge is presented as a core element of deterrence of enemies in different arenas). In the Israeli cyber security strategy, while technology does not appear as a core principle, it is one of three overarching efforts for implementing the overall strategy, that is, one of the components of Israeli cyber defense strength.

Furthermore, each of the three strategies places a detailed emphasis on continuing force buildup via technological R&D. The dedicated description in each one of the strategies highlights the central role that each document ascribes to technology. Likewise, the three strategies emphasize that the technological advantage is based on appropriately trained human capital.

At the same time, the essential difference in the discussion of technology is that only the cyber security strategy comprehensively addresses "how" to maintain the technological edge and not only "what" is necessary. In the *Israel Cyber Security Strategy*, there are overall strategic guidelines for maintaining the technological edge, which is one of the means for achieving the overall ends, but given its deep significance it is a sufficiently important means to justify the description of a mini-strategy of how to maintain it. This mini-strategy is incorporated throughout the document and stands out particularly in the supporting effort for "national scientific-technological cyber force buildup" (National Cyber Directorate, 2017, pp. 42-46). The overall end is quality force buildup for cyber defense, or in other words, maintenance and enhancement of Israel's technological edge in cyber security, and more. The discussion of cyber force buildup at a national level relates to the aspect of national security in its broad sense in the cyber world, that is, force buildup at the level of a power as a national-security tool and not only for the sake of cyber defense of the state. The ways are efforts to translate human capital for a technological edge, such as incorporating academia and industry, or the efforts to enlarge human capital and improve its quality; and the means are the human capital itself, resources, academia, industry, and so on.

Some may claim that the cyber security strategy discusses a relatively specific issue in depth in comparison to the two other security strategies, and therefore there is room in this strategy for further description and deep discussion of specific issues. However, similar strategies in other countries do not necessarily relate to technology in this broad manner, and only discuss direct cyber defense of the state. In that sense this strategy is unique, both globally and in Israel, particularly in its discussion of the technological aspect, which is the very element that lies at the center of the qualitative edge (Adamsky, 2017).

Part II: Foreign Security Strategies

The role of technology in Israeli strategies can also be viewed against the role of technology in two foreign security strategies: *The National Security Strategy of the United States of America*, published in December 2017 during the administration of President Trump (White House, 2017),[3] and the *National Security Strategy of the UK*, published in 2015 (HM Government, 2015). The United States and United Kingdom were chosen for this comparison as they are indisputably leading global security and technology powers. The two documents are comprehensive and deal with a variety of issues relating to the national security of these countries at the widest scale, including, for example, discussion of how to manage specific threats such as terror and crime, global and regional interests, international diplomacy, and issues in the economic context; they also discuss the scientific-technological subject extensively.

The United States National Security Strategy

The National Security Strategy of the United States of America is published by each new administration once every four years (the first such document was published in 2002). It describes the administration's view of US national security issues and how to address them. The document analyzed in this article was published in December 2017 during the administration of President Trump (White House, 2017).

In the 2017 document, technology figures on a number of levels. First, technology is presented as a central component of strengthening and furthering the prosperity of the US economy; in other words, technology is discussed in the national context as a tool for maintaining a civilian-economic edge, in contrast to the explicit military context in which it appears in Israeli strategies. Later, the document presents the security contexts of technology and its role in maintaining the United States' qualitative military edge over its rivals (ends), which is eroding over time: "A belief emerged, among many, that American power would be unchallenged and self-sustaining. The United States began to drift. We experienced a crisis of confidence and surrendered our advantages in key areas. As we took our political, economic, and military advantages for granted, other actors steadily implemented their long-term plans to challenge America and to advance agendas opposed to the United States, our allies, and our partners" (p. 2). Regarding both economy and security, the document presents methods to maintain the technological qualitative comparative edge (ways), which in many senses overlap and rely on the same building blocks—scientific and technological manpower, innovation, entrepreneurialism and prioritization of technologies, investment in R&D, development of a scientific and technological knowledge infrastructure, and domestic and international cooperation. The document discusses each of these subjects in depth and describes the means to advance and strengthen them.

On scientific and technological manpower, the document presents the need to advance scientific and technological education, and especially to strengthen STEM subjects (Science, Technology, Engineering, Mathematics), and to cultivate academic manpower with technological specialization and professionalization. Specifically regarding the security sector, the document suggests recruiting technologically-trained, innovative, inventive human resources; removing obstacles and offering incentives for recruiting federal STEM employees; and offering salaries that compete with the civilian job market, in order to create easier paths of entry for tech professionals, scientists, and engineers into the public sector (pp. 19-20).

The document includes a section (pp. 20-22) dedicated specifically to innovation and defines the central purpose of this field as maintaining global leadership in technology inventions and innovations, in order to maintain the American competitive edge. This section emphasizes prioritizing essential technologies for economic growth and security, particularly artificial intelligence, and monitoring scientific and technological development trends around the world in order to understand how these are likely to influence the United States or undermine US programs and strategies. This section also discusses how to leverage the private sector and its expertise in building and innovation. The document notes the need for regaining the element of surprise in the technological field by integrating new technologies on the battlefield at the pace of modern civilian industry, while promoting risk-taking.

The *Strategy* discusses the need to improve R&D and invest in it from earlier stages, to enhance effective use of R&D and the expertise built by the private sector to meet national economic and security needs, and to promote and defend the National Security Innovation Base.[4] The document particularly emphasizes the need to defend American knowledge in the security field, which typically grows out of academia and various civil industries and is essential for maintaining the qualitative edge. It also addresses (pp. 22-23) the need to invest in energy technology in order to achieve energy independence and address air pollution and climate impact; this highlights the role of technology in dealing with global problems and creating energy independence, including nuclear energy.

On the subject of cooperation, the *National Security Strategy* repeatedly emphasizes the importance of external technological collaboration with allies and partners, and domestic collaboration between the US government, industry, and academia. Likewise, it states the importance of strengthening the connection between the security system and civilian tech companies as a central point of leverage for promoting technology at the national security level. The document discusses tech capabilities as a tool with hard and soft power potential, and a tool to maintain and create influence to counter global threats that rely on technology (pp. 25-26). It discusses technology in the hands of the superpower's enemies, which reduces and erodes the clear American technological edge (p. 3).

However, the document also expresses reservations about complete dependence on technology and argues that the dependence and complete faith in technology as the element that can compensate for the balance of power was mistaken: "We also incorrectly believed that technology could compensate for our reduced capacity—for the ability to field enough forces to prevail militarily, consolidate our gains, and achieve our desired political ends. We convinced ourselves that all wars would be fought and won quickly, from stand-off distances and with minimal casualties" (p. 7). The *Strategy* insists that alongside dependence on technology, military capabilities must be renewed and modernized, there must be massive acquisitions of arms, and force sizes must be increased (p. 29).

The UK National Security Strategy and Strategic Defence and Security Review

The National Security Strategy and Strategic Defence and Security Review of the United Kingdom was first published in 2008; two updated documents were published since then, most recently in 2015 (HM Government, 2015). Like the American document, this document describes national aims for the UK in the field of security, challenges to British national security, and ways to address them.

This document likewise describes in a highly comprehensive manner the centrality of technology in national security. It shows how technological advances around the world, particularly in the fields of IT and cyber, impact national security significantly and present both an opportunity and a threat; it also illustrates how technological progress in a variety of areas has enormous potential in the economic and security fields (p. 19). The document claims that a security industry that promotes innovation and competitiveness is a central element of addressing threats to the UK's national security. Innovation in the products and services supplied by the security industry allows the maintenance of a competitive edge over opponents. The document also discusses the scale of Ministry of Defence investment in science and technology.

The UK *Review* describes what should be mandatory investments in advanced security capabilities—jets, cyber, space, communications, counterterror, and more—along with strategic cooperation with friendly nations and partners, such as a collaboration with France in developing unmanned aerial vehicles. Regarding all these capabilities, significant technological investments are necessary to maintain a competitive relative advantage, while consolidating scientific and technological knowledge and R&D through military-civilian-industrial partnership.

Like the American document, the *Review* has a specific section dedicated to innovation (pp. 73-75), which notes that innovation relies on making use of scientific and technological capabilities essential for UK economic power, productivity, and competitiveness in the global market. It also notes that in the world of technology today, the private sector and not the public sector is the driving engine, and that cooperation between the private technological sector and the public one is a key component of the full use of technology for national security. For example, the document presents the launch of a national defense innovation initiative that will work with universities, start-ups, and small and medium-sized enterprises, while making science and technology central to national security thinking: "We will create a new, cross-government Emerging Technology and Innovation Analysis Cell, with close links to the private sector and academia to ensure that we identify these opportunities" (p.74).

The document also announces (p. 74) investments in innovative technologies with the potential to disrupt opponents—which includes advanced research in the Ministry of Defence's Science and Technology Laboratory and the Home Office's Centre for Applied Science and Technology, along with close work with industry and academia. In this context, it discusses the need to advance technology rapidly, explore unconventional ideas, and be willing to take risks and change traditional mindsets. The document also relates to commercialization of capabilities developed for security purposes, to further economic growth in fields such as cyber, and to establish a security accelerator to assist all sectors in turning ideas into innovative products and services more quickly and delivering them to security users (p. 75).

The document addresses the need for the government to define which technologies it must develop by itself, and which it must purchase externally or develop in cooperation with allies, academia, and industry via shared investments (make-or-buy) (p. 74). For example, it discusses strategic technological collaboration between the UK and the US as a central component of national security, alongside cooperation in intelligence, nuclear, diplomatic, and military capabilities, as part of the American “Third Offset Strategy” (Shmuel, 2016), and cooperation with France with technological initiatives in aviation, sea, and space. The document specifically discusses sharing technological knowledge as an element of strengthening security relations (p. 75).

In the context of technological manpower, the document explains the necessity of developing and cultivating technological manpower (STEM and entrepreneurship); easing mobility between academia, the private sector, and the security sector and between countries; advancing the security industry and security exports; and positioning security industries as advanced, innovative, and competitive, including incorporating new and sometimes small companies in the security field, and including reducing limitations on sales and exports (pp. 75, 78).

Technology has an extremely central place in the national security doctrines of the two Western national security strategies discussed here.

The UK *Review* was preceded by *National Security through Technology*, which the Ministry of Defence published in 2012 (Ministry of Defence, 2012). Over the course of 65 pages the document describes the ways to achieve a relative edge, while the end of the plan is to provide the armed forces and security agencies with the best means available given budgetary limitations, over the short and long term, with a proactive and initiative-taking approach.

Comparison between Foreign and Israeli Security Strategies

Technology has an extremely central place in the national security doctrines of the two Western national security strategies discussed here. They examine the technology field in a comprehensive fundamental way with the three components of strategy (ends, ways, means)—technological targets and methods to achieve them in order to meet national security targets, and ways and means to achieve and maintain the technological edge. The two strategies find technology to be so important that they define it as an end in itself and not only as a way to achieve security; in other words, they define it as a central component of national security on its own, and discuss its importance for a thriving economy as well as for a secure country. In this manner they differ fundamentally from Israel’s strategy, which, although it perceives technology as an important element of national security, does not define it as an end in itself, but rather as a way to achieve other ends. (The exception to this is in the field of cyber, where Israel has a significant global footprint.)

The two foreign strategies describe the ways to promote national security technology, such as strengthening relations between the Ministry of Defense, industry, and academia; collaborating domestically and internationally; establishing innovation centers and security tech accelerators; developing groundbreaking tech knowledge and using it to strengthen collaboration and security ties while preserving unique advanced knowledge; advancing security exports; and implementing make-or-buy decisions. The two strategies also describe the means to promote technology, such as development, cultivation, and mobilization of tech manpower and substantial financial investments in science and technology. The foreign strategies thus offer a broad look at the role of technology along the entire value chain (technology and science education, technological manpower, R&D bodies) and the complete ecosystem needed to create and maintain it, and consider how to act in order to maintain tech leadership over time.

In contrast, the Israeli strategies that address the tiers of national security and military defense present a very partial picture of the ways to achieve technological targets as part of overall strategic thinking, which creates a conceptual and theoretical disparity between aims and means. This disparity leads to incomplete, imbalanced strategies and flaws in what is written about the central place of technology within these strategies. The cyber security strategy deals with ways to achieve the technological edge, i.e., by addressing ends, ways, and means and offering a broad overall outlook although not in the same depth as in the foreign strategies.

Furthermore, the foreign strategies deal extensively with resources (budgets, manpower, establishment of bodies, and frameworks) for implementing the ways to strengthen the technological edge. Such a discussion is lacking from the first two Israeli strategies and appears only partially in the cyber security strategy (which does not mention budgets, for example). The subject of scientific and technological cooperation within these countries and with allies is also a central element of their strategic outlook, but is lacking from the Israeli strategies almost entirely.

The practical implication of the strategies and the role of technology are also evident: from the national security strategies come written working documents about how to maintain the technological edge, such as the "National Security through Technology" in the UK and the "Third Offset Strategy" in the US (Shmuel, 2016), and carried out by the Department of Defense and other bodies.

Part III: Discussion

Technology has been one of the central components of security concepts and modern strategies over recent decades, particularly in the West, and recognized as a central tool for maintaining a qualitative comparative edge. As such, it sometimes even appears not only as a way to achieve various ends but also as an end in itself.

In addition, an examination of security strategies reveals that technology is, naturally, one of the means to fulfilling security ends, but in many senses can also have a fundamental influence on the ways to achieve these aims. For example, the Iron Dome system is not just a means for addressing the rocket threat, but by its very existence and successful interception of a large proportion of rockets fired, changes the combat strategy of the IDF to a defensive strategy (ways).

Furthermore, technology can also influence the ends themselves. For example, as cyberspace, which is a fundamentally technological space, became a security domain, security ends changed, and not only the ways to achieve them. Accordingly, a new security end was born of defending vital infrastructure from cyberattacks. When discussing the lower level of technology strategy in itself, maintaining the qualitative edge can be considered the end of the tech that we want to develop or possess. We must thus develop, prioritize, cooperate, and take make-or-buy decisions about development or purchase/import, and decide on additional ways and means such as budgets, infrastructure, and manpower.

Gaps in Israeli Security Strategies

Israeli strategic security concepts clearly view technology as an important and central component of creating and maintaining Israel's qualitative comparative security edge, which is one of the essential elements of Israeli security strength on the levels of national security and direct defense, both in practice and in written documents. They thus incorporate a detailed description of "what" is necessary from such technology, while relating to required tech capabilities.

These strategies, however, and particularly the IDF and national security strategies, do not sufficiently deeply discuss "how" to maintain a technological edge, as would be expected from strategies that emphasize the importance of technology. This is even more clear in comparison to the strategies' discussion of other issues. This shortcoming is less pronounced in the cyber security strategy, though not as detailed as the US and UK national strategies. The three Israeli strategies, with their respective differences and emphases, do not explore with sufficient depth the most essential questions regarding investments over the long term. These include the correct policy for strengthening Israel's comparative advantage, and how to overcome weaknesses in this field; when should policy aim at independent development and when should it rely on technologies produced abroad; where should civilian technologies be relied on and where should security establishment R&D or military industry development be strengthened—and what are the differences between the latter two; and how should this advantage be translated into military power. In other words, missing is a deep examination of national security force buildup processes.

With respect to the national security strategy, there is a lack of discussion of the creation of a complete ecosystem of cultivating scientific-technological human capital, the place of academia in this national force buildup, and how it can be strengthened at a national level, including from the perspective of national security, R&D, and so forth, to create military strength. Promoting civilian scientific and technological research as a component of national security, maintaining the civilian-economic advantage and competitiveness on the global market, and expanding and easing movement between the public and security sectors and the civilian sector should also be addressed. These gaps are especially pronounced in comparison to the comprehensive discussions of technology in the US and UK national security strategies. It is puzzling that the State of Israel, for which science and technology are core pillars of its economy and its military and political strength today, does not have a comprehensive discussion in the context of its national strategy, or in a national technological strategy approved by the government.

Is Practice More Important than Theory?

One may argue that strategy is less important than practice and what matters is action, based on the claim that Israel managed to create its scientific-technological strength without a clear written strategy, just as its national security outlook is also not formalized in any binding document.

Nonetheless, various bodies bother to write strategies because there is an importance to written strategic documents in general, and in particular to formal security doctrines. First, they constitute a shared framework for all those who deal with operational planning and force buildup, and for all partners in the security effort, because they create a coherent and clear outline of ends, ways, and means, so that all involved know where to focus their efforts and what part they play in the whole. Second, these strategies are particularly important for decision making, not only about what should be done but also on what to exclude. The lack of any of these elements in a strategy may lead to overstretching, allocating resources and efforts in an unfocused way, and making significant and critical mistakes. Likewise, strategies influence the practical allocation of resources, manpower, and priorities on the basis of that which should be done. Finally, the written content of strategies reveals the way that senior state and security system decision makers think and the depth of their thought.

Thus, the importance of writing national strategies is clear, and the element of technology is no exception. From the manner in which technology is discussed in Israel's security strategies it is clear that the technological edge is perceived mainly as a means toward deterrence of enemies and decisive victory when needed, but not as a strategic end in itself that requires building an underlying strategy. Furthermore, it seems that there is a hidden assumption that the cultivation and maintenance of the technological edge can be taken for granted and will occur as a byproduct regardless—particularly in the *IDF Strategy*. This assumption among decision makers may result from Israel's being an advanced technological state with a strong tech industry, in which the civilian market produces and advances many technologies, mainly for export, that also influence the military framework that benefits from the fruits of industry. This impression is heightened by the fact that Israel's security doctrine omits the connection between technology on the civilian market (as a means to maintain a civilian-economic edge) and the security technology edge. In contrast, the US and UK national security doctrines address this connection explicitly.

Strategic Civilian Leadership

Does the fact that senior Israeli security decision makers usually come with an operations background, and typically have no technological or scientific training, have a direct impact on the relative absence of technology from the strategies? Perhaps, though not necessarily. Israel's first Prime Minister, David Ben Gurion, who did not have a formal technological background, saw science and technology as the basis for the establishment of Israel and a central component of its national security in both the broad and the immediate military senses. He worked ceaselessly to advance them and expressed this clearly in both his writings and his actions (Ben-Israel, 2013). The central role he assigned scientists in the security system and his personal involvement in the establishment of the science headquarters and the IDF Science Corps during the War of Independence (Barel, 2009) was a central factor in making technology an essential element of Israel's national security (Matania, 2022).

Ben Gurion was not the only proponent of the view that scientific and technological action are essential components of Israeli strength. There were other decision makers and strategic leaders whose affinity for science and technology, comprehension of the importance of these fields, and decisions on the subject were noteworthy: Shimon Peres (i.e., in nuclear research); Yitzhak Rabin (i.e., in promoting the vision of satellites in spite of IDF opposition, due to understanding the overall long-term political implications of the field for national security); Moshe Arens (particularly for independent R&D); and Benjamin Netanyahu (for example, in the cyber realm, where he pushed for Israel to be a world leader, not only in relative terms but absolutely; it is the first technological field in which Israel became such a leader [Matania & Rapaport, 2021, p. 14], while sometimes being perceived as obsessive). All had curiosity and thirst to understand the technology realm, had an affinity for technology, or developed technological intuitions over the course of years of contact with the tech field, which allowed them to consider and make decisions about security technology.

> Israel's first Prime Minister, David Ben Gurion, who did not have a formal technological background, saw science and technology as the basis for the establishment of Israel and a central component of its national security in both the broad and the immediate military senses.

That said, most of these decisions were decisions about a particular issue at a particular point in time, which required major investments and budgets at a national level, and thus required a principled decision by senior leaders of the government and security system. The particularity of these decisions made them the exception that proves the rule—there is no broad overall strategy for technology.

The Need for Leadership with Technological Savvy

An additional surprising phenomenon in relation to the future of technology in Israel—a country where technology is a central component of the economy and of national security—is the small number and sometimes the complete absence of tech specialists or people with a serious affinity for or understanding of technology in strategic decision making forums. In the security establishment in particular, this situation has implications for the depth of strategic thinking on this matter, on the ability to make critical decisions about technological force buildup and priorities, and on proper allocation of resources. How many of those sitting at the IDF General Staff table understand or have knowledge of technology and how to use it correctly in force buildup and application? How can commanders of IDF forces who are not technologically savvy or experienced fully understand technological changes that disrupt various combat capabilities and change them fundamentally, and prepare the forces they command for these changes, in which manned platforms will no longer necessarily be the primary ones? How many directors in the Ministry of Defense, with the exception of the head of the Directorate of Defense Research and Development (DDR&D), are capable of making decisions in the technology field? How many in the government?

This is perhaps one of the conclusions that should be drawn from this study. It is important, if not necessary, that those responsible for Israeli's strategic doctrine and national security will develop technological knowledge and intuition over the years, whether on their own initiative or in accordance with a directive to undergo training in this field.

Technological Strategy for Israel

The comparison to the national security strategies of the United States and the United Kingdom underscores that the Israeli strategic environment must formulate a comprehensive national security technology doctrine, as an accompanying document to the existing strategy documents. Formulating an overall strategy will continue to strengthen the scientific-technological component of national security doctrine and maintain and cultivate Israel's qualitative technological comparative advantage, as part of the state's official security doctrine.

Such a strategy must be comprehensive, relate to the central ends of how to maintain the defensive and civilian technological edge, and link them to ways and means to achieve them. Such a strategy must relate to central dilemmas regarding technology. These include how to divide responsibility in the civilian and defense technology ecosystem (e.g., who is responsible for leading and making decisions regarding technological manpower development in the state); how a complete ecosystem looks; how to cultivate both civilian and defensive manpower; how to cultivate a scientific and technological knowledge base; how to create collaboration between the security establishment, industry, and academia; how to translate the technological edge into military power; what are appropriate budgets for investment in R&D; what is the correct balance between purchasing Israeli and American arms; and so on. There is a gaping lack of discussion of these issues in the existing security strategies, yet they are decisive in maintaining Israel's technological edge over time.

Conclusion

Since its establishment, the relative qualitative edge of the State of Israel, including its technological component, has been a central and important element in its security outlook. This work examines how technology was formally discussed in Israel's security strategies over the past two decades, and whether the formal expression of this thinking corresponds with the significance of technology in security doctrine. Written strategies of this sort will significantly influence the future of the field in the coming decades: they create motivation among all relevant parties, point toward strategic direction and focus for decisions (what to do and what not to do), highlight efforts, priorities, choices, and resources, and outline a shared national vector and consistent address of this vital component in Israel's national qualitative edge. Such a perspective is not the only important or the complete one, but it enables drawing singular critical conclusions.

To this end we focused on three national strategies published over the past two decades: the National Security Doctrine (Meridor Committee), which discussed the highest tier of national security, even if it examined security narrowly without relating to social resilience or economic power; the *IDF Strategy*, which examined the military-defense level, one level below that of national security; and the *Israeli Cyber Security Strategy*, which deals only with one national issue but discusses it from both a national security and a direct military-defense perspective. These strategies were examined from a number of directions: the role of technology in the documents themselves was compared to what would be expected from a strategic document, particularly in comparison to other issues they discussed (a normative view); the role of technology was studied in a comparative analysis; and these findings were compared and analyzed against the US and UK foreign national security strategies.

The central conclusion is clear: There is a substantial disparity between the existing formal discussion of technology as a prominent, central, important factor in Israeli security strength, and the formal discussion of ways to achieve and maintain this end. Strategically this disparity is most pronounced in the glaring lack of a comprehensive strategy for maintaining a comparative technological edge, enhancing it, and translating it to defensive and security strength in practice over time. Such a lack may result from a number of factors, including the view of technology as a means and not an end, and a hidden assumption that technology can be taken for granted, perhaps as a result of the influence of the civilian advanced technology market in Israel or from a shallow understanding of this issue among senior national security establishment officials.

Technology, however, must be examined from a strategic outlook as an aim and end in itself, and not only as a means to achieve other national and military ends. This is critical in light of its centrality and importance to Israel's national security from a broad perspective, including impact on the economy, and not only direct security impact. Such an examination requires formulating an overall strategy to maintain and cultivate the Israeli qualitative technological edge over time and to maintain national security strength.

Technology must be examined from a strategic outlook as an aim and end in itself, and not only as a means to achieve other national and military ends.

Prof. Eviatar Matania is a professor in the School of Political Science, Government, and International Affairs at Tel Aviv University. He directs the MA Security Studies Program and the MA Cyber Politics and Government Program, and directs the Research Center for Air and Space Studies. During the years 2012-2018 he founded and directed the National Cyber Directorate. eviatarm@tauex.tau.ac.il

Oren Podhorzer and Nir Daniel were student researchers in the MA Security Studies Program at Tel Aviv University.

References

Adamsky, D. (2017). The Israeli odyssey toward its national cyber security strategy. *Washington Quarterly, 40*(2), 113-127. DOI: 10.1080/0163660X.2017.1328928

Amidror, Y. (2020). Israel's national security concept. *Bein Haktavim 28-30*, 19-34. https://bit.ly/3AOBV6S [in Hebrew].

Barel, A. (2009). The leader, the scientists, and the war: David Ben Gurion and the establishment of the science corps. *Israel: Journal for the Study of Zionism and the State of Israel— History, Culture and Society, 15*, 67-92. https://bit.ly/3x1lofE [in Hebrew].

Ben-Israel, I. (1997). The theory of relativity of force buildup. *Maarachot, 352-353*, 33-42. https://bit.ly/3LxQMGm [in Hebrew].

Ben-Israel, I. (2013). Israel's security doctrine. Broadcast University, Modan, Ministry of Defense Publishers [in Hebrew].

Ben-Israel, I., Matania, E., & Friedman, L. (Eds.). (2020). The national initiative for secured intelligent systems to empower the national security and the techno-scientific resilience: A national strategy for Israel—Special report to the Prime Minister. Tel Aviv University, Yuval Ne'eman Workshop for Science, Technology and Security.

Cancian, M. F. (Ed.). (2017). *Formulating national security strategy: Past experience and future choices*. Center for Strategic and International Studies (CSIS). https://bit.ly/3TGUItp

Eilam, U. (2009). *Eilam's arc: How Israel became a military technological powerhouse*. Yediot Ahronot and Hemed—Maskel Books [in Hebrew].

Finkel, M., & Friedman, Y. (2016). Seven decades of the IDF qualitative edge: Changing outlooks on the essence of the IDF's qualitative edge over its enemies, changes in the qualitative edge in practice and future directions. *Bein Haktavim 9*, 43-66. https://bit.ly/3q94bfw [in Hebrew].

Hamo, Y. (2016). Force buildup as a campaign: On optimization and strategy. *Bein Haktavim, 6*: Force Buildup, Section A, 11-38. https://bit.ly/3CVfvU4 [in Hebrew].

HM Government. (2015). *National security strategy and strategic defense and security review 2015: A secure and prosperous United Kingdom*. https://bit.ly/2vlh1hb

IDF Strategy. (2018). IDF website. https://bit.ly/3enE0yW [in Hebrew].

Matania, E. (2022). Behind mandatory service in Israel: From the rationale of the militia to the rationale of military-technological superiority. *Strategic Assessment, 25*(2), 3-23. https://bit.ly/3ilGeRj

Matania, E., & Rapaport, A. (2021). *Cybermania: How Israel became a global powerhouse in the domain that is revolutionizing the future of humanity*. Cybertech-Arrowmedia Israel Ltd.

Meridor, D., & Eldadi, R. (2019). *Israel's National Security Doctrine: The Report of the Committee on the Formulation of the National Security Doctrine (Meridor Committee), Ten Years Later*. Memorandum 187, Institute for National Security Studies. https://bit.ly/3VGCWH0

Ministry of Defence. (2012). *National security through technology: Technology, equipment, and support for UK defence and security*. https://bit.ly/3RgJqdf

National Cyber Directorate. (2017). *Israel cyber security strategy*. https://bit.ly/3PPkMzi [in Hebrew].

Rounds, R. K., III. (2019). *Sourcing air supremacy: Determinants of change in the international fighter jet network* (Doctoral dissertation). Georgetown University. https://bit.ly/3cNRDHj

Shmuel, S. (2016). 2012-2016: The journey to the third offset in the American security establishment. Dado Center. https://bit.ly/3qdkBne [in Hebrew].

White House. (2017). *National security strategy of the United States of America*. https://bit.ly/3e41d95

Yarger, H. R. (2006). Toward a theory of strategy: Art Lykke and the US Army War College strategy model. in J. B. Bartholomees, Jr. (Ed.), *U.S. Army War College guide to national security policy and strategy,* 2nd ed. (pp. 107-114). https://bit.ly/3Rh5ogP

Notes

[1] Some parts of the *Israel Cyber Security Strategy* that required Israeli government authorization for establishment or operation were authorized by the government at several points in time, particularly Government Decisions 2443 and 2444 from February 15, 2015.

[2] Full disclosure: Eviatar Matania, one of the authors of this article, led the development and writing of the Israeli cyber security strategy in the framework of his role as the founder and director of the National Cyber Directorate.

[3] The Biden administration published the latest *National Security Strategy of the United States* in October 2022. That document is beyond the scope of this study.

[4] The National Security Innovation Base, an American network of knowledge, capabilities, and people that includes academia, national laboratories, and the private sector, turns ideas into innovation and discoveries into commercial products and companies.