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

Israel:
The Making of a Global Cyber Power

Matthew S. Cohen and Charles (Chuck) D. Freilich

Mideast Security and Policy Studies No. 209

THE BEGIN-SADAT CENTER FOR STRATEGIC STUDIES
BAR-ILAN UNIVERSITY
Mideast Security and Policy Studies No. 209

Israel:
The Making of a Global Cyber Power

Matthew S. Cohen and Charles (Chuck) D. Freilich

Israel: The Making of a Global Cyber Power

Matthew S. Cohen and Charles (Chuck) D. Freilich

Bar-Ilan University
Ramat Gan 5290002 Israel
Tel. 972-3-5318959
Fax. 972-3-5359195
office@besacenter.org
www.besacenter.org

ISSN 0793-1042
October 2024

Cover image: Shutterstock

The Begin-Sadat (BESA) Center for Strategic Studies

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

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

Israel:
The Making of a Global Cyber Power

Prof. Matthew S. Cohen and Prof. Charles (Chuck) D. Freilich

EXECUTIVE SUMMARY

Israel, a country with the population of New York City, has become one of the world's top cyber powers. Five primary factors account for this: the symbiotic relationship between the IDF and Israel's commercial cyber sector, academia, and government ministries; compulsory military service in the IDF; the IDF's singular contribution to the training of Israel's cyber experts; cyber education; and a unique national culture, what we call "chutzpah gone viral."

This study draws on Israel and the Cyber Threat: How the Start-Up Nation Became a Global Cyber Power*, by Charles D. Freilich, Matthew S. Cohen and Gabi Siboni, Oxford University Press, 2023. Permission to use this material is acknowledged with gratitude.*

Prof. Matthew Cohen is an Assistant Professor of Practice in the Political Science and Public Policy Department at Merrimack College in North Andover, Massachusetts. He earned his PhD in Political Science at Northeastern University. Matthew previously served as a consultant for the Cyber Security Project at Harvard University's Belfer Center for Science and International Affairs. He has previously published on cyber-security policy, Russian foreign policy, international relations theory, delegitimization and lawfare, Israeli security policy, Turkish-Israeli relations, and Turkish politics.

Prof. Charles (Chuck) Freilich, a former deputy national security adviser in Israel and long-time senior fellow at Harvard's Belfer Center, is a senior fellow at the MirYam Institute and INSS in Israel. He teaches political science at Columbia University, NYU, and Tel Aviv University. He is the author of Zion's Dilemmas: How Israel Makes National Security Policy *(Cornell Press 2012) and* Israeli National Security: A New Strategy for an Era of Change *(Oxford Press 2018 and Modan Press in Hebrew). Chuck is senior editor of* Israel Journal for Foreign Affairs *and has published numerous academic articles and over 220 op-eds.*

Israel was one of the first states to awaken to both the threats and opportunities presented by the cyber era. Over time, the cyber realm has come to pervade nearly every facet of Israeli national life and become both a primary engine of economic growth and an important area of military advantage. Astonishingly, Israel – with just 0.001 of the global population – is home to as many cyber startups as the rest of the world combined, not including the United States.

Cyber is, however, also the source of potential new vulnerabilities. Israel is far more cyber-dependent than its adversaries and therefore more vulnerable to attack. In practice, Israel faces a nearly constant barrage of cyber-attacks. In early 2023 alone, Israel blocked more than 1,000 attacks that had the potential to cause significant economic disruption. In the early months of the war against Hamas in Gaza, there were some 3,400 significant attacks, more than double the multi-year average for that period.

Nearly every possible type of computer system in Israel has been attacked, including critical infrastructure firms (electricity, water, communications). The IDF and intelligence community have also been central targets and have faced numerous attempts to break through their defenses and penetrate computer systems, including operational ones. The intensity of cyber-attacks against Israel has been shown to increase significantly during periods of both heightened military tensions and diplomatic activity.

In addition to cyber, Israel faces myriad military threats, and its largely reservist military has exceedingly short mobilization times. A cyber-attack that disrupts power, communications, or transportation systems, even briefly, could make a critical difference in times of war. Even something as basic as the shutting off of traffic lights could delay the mobilization of forces and have a significant impact on military operations.

Israel's response in the cyber realm has thus been a matter of strategic necessity. However, cyber is also "made to measure" for Israel and is viewed not just as a strategic and socioeconomic imperative but as an opportunity. Indeed, Israeli society has traits that are particularly well suited to the cyber realm, some drawing on Jewish traditions and experiences and others more uniquely Israeli.

Among these traits is a deeply ingrained societal propensity to challenge authority and reject accepted norms, practices, and wisdom – to refuse, in other words, to take no for an answer and to search instead for alternative solutions. This fundamental societal characteristic is further strengthened by the heterogeneous nature of Israeli society, which consists of immigrants from over 70 national and cultural backgrounds. Immigrants, by nature, tend to be entrepreneurial and willing to take risks. Israeli society has also always been characterized by its unusually non-hierarchal and informal nature. These societal characteristics are typical of successful high-tech firms in general and cyber firms in particular.

Compulsory military service enables the IDF to harness the talents of Israel's very best and brightest. In the cyber realm, just a few geniuses can make all the difference. Many of the IDF's top talents were already employed by high tech firms while still in high school, and their skills are in great demand. To find them, the IDF scours Israel's high schools long before students begin their military service and conducts intensive screening processes.

Compulsory military service also means that the total cyber personnel available to the IDF approaches that of global powers. Whereas the American National Security Agency, for example, has approximately 40,000 personnel, Israel's equivalent, Unit 8200, reportedly has as many as 10,000. Smaller, but not by orders of magnitude.

The IDF's critical need for highly trained and innovative personnel has made it one of the driving forces behind cyber education in Israel. In addition to providing support for educational programs in the public school system, a variety of IDF units provide training programs for approximately 10,000 soldiers a year in cyber-related areas.

Cyber has partially upended the regional balance of power in the Middle East, providing Israel with important economic and military advantages. Access to Israel's cyber capabilities was one of the reasons why the UAE, Bahrain, and Morocco normalized relations with Israel in 2020 (the Abraham Accords), and the desire for similar access is behind Saudi Arabia's and other Arab states' increasingly close ties with Israel. Cyber has also been an important component of improved ties with countries of great importance for Israel, such as the UK, India, and China.

Israel's offensive and defensive cyber capabilities have become important components of its military might, as have its cyber-based intelligence capabilities. In a world increasingly averse to human losses and in which Israel is excoriated for allegedly disproportionate uses of force, cyber provides an important means of achieving at least some military objectives without loss of life and property, thus reducing the risks of retaliation and escalation. No other Middle Eastern state has a digital economy and cyber ecosystem as advanced as Israel's; nor have any of them applied cyber technologies for military purposes to the extent that Israel has. As in other areas, the US is Israel's primary partner in the cyber realm.

Introduction

Israel, a country with the population of New York City and the geographic size of New Jersey, has become one of the world's top cyber powers in the civil and military realms alike. In the 1990s, when the cyber era began to dawn, Israel was one of the first states to awaken to both the threats and the opportunities it presented. Since then, the cyber realm has come to pervade nearly every facet of Israeli national life, including economic, social, cultural, governmental, diplomatic, and military aspects. Indeed, cyber has become a primary engine of Israeli economic growth and an important area of military advantage. Today, Israel is ranked at the forefront of the cyber realm. It is a second-tier global cyber actor alongside Russia, China, and the UK, just below the first-tier United States.[1]

Israel has just 0.001 of the global population, but astonishingly, it is home to as many cyber startups as the rest of the world combined, not including the United States. Israel's economy is the most tech-dependent in the world and Israel is a global leader in overall high-tech R&D and startups, per capita.[2]

To understand why and how this happened, we must begin by placing it in the broader context of Israel's strategic culture and the threats and opportunities that sparked Israel's interest in the cyber realm to begin with.

Part I: Threat, Opportunity and Strategic Culture: Why Israel Became a Cyber Power

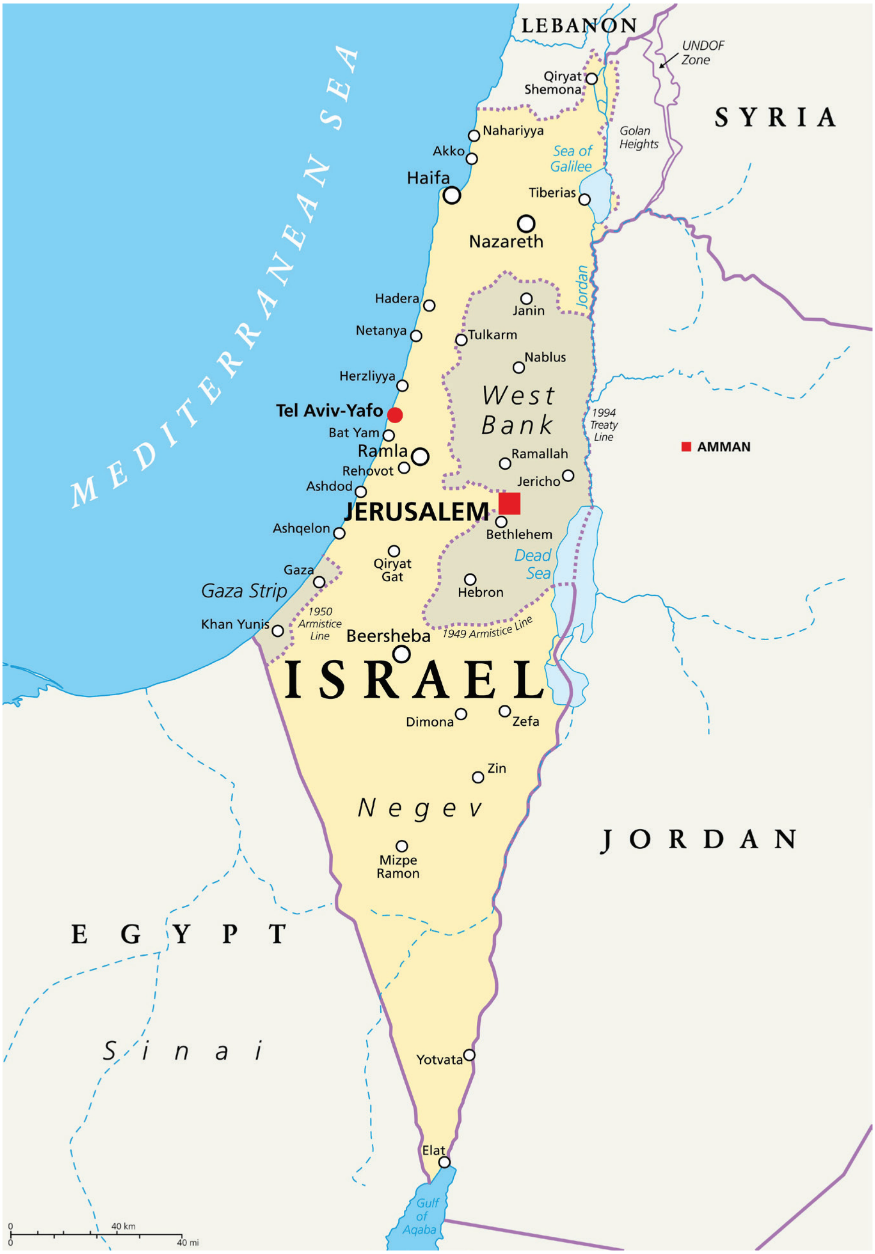
Strategic culture refers to a nation's historical beliefs, collective memories, values, traditions, and strategic assumptions.[3] Strategic culture is not destiny and does not predetermine a state's policy choices, but it does have an important impact on the decision-making processes that shape them.

Understanding Israel's strategic culture requires an appreciation of the country's unique national mindset and the historical burden that weighs heavily upon it. Israel is not just another state, but the embodiment of a 2,000-year-long yearning for national revival. The Jewish people's long history of suffering discrimination and persecution, which reached its genocidal climax in the Holocaust, imbued Israel's national psyche with a fundamental sense of insecurity. From its founding, Israel has viewed itself as a state under siege, encircled by enemies openly avowed to its destruction with far greater populations, resources, and military power. Arab enmity was believed to be so unremitting and immutable that to merely thwart their efforts to destroy Israel would be insufficient to achieve deterrence and ensure its security. This magnified the historic sense of insecurity and led to the basic Israeli assumption – still very much relevant today – that the nation faces an ongoing existential threat.

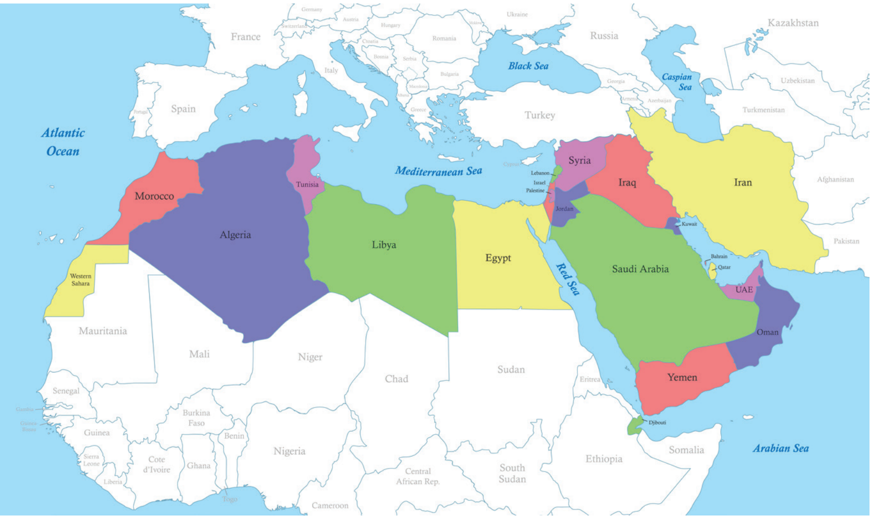
The resulting "Masada Complex" or "Holocaust Syndrome" reflects this primal fear and consequent national preoccupation with security. It is the primary factor shaping Israel's identity, strategic culture, and national security policy. "Our fate in the land of Israel", Prime Minister Menachem Begin famously warned, "is that we have no choice but to fight with selfless dedication. The alternative is Auschwitz." Prime Minister Benjamin Netanyahu has similarly drawn repeated comparisons between the Germany of 1938 and the Iran of today.[4]

Israel's narrow and elongated geography is a strategic nightmare. Israel is tiny, at slightly over 7,700 miles^2 (20,000 km^2) within the 1967 borders and 9,960 miles^2 including the West Bank (23,600 km^2). Some 70% of the population and 80% of the economic base, along with most government institutions, strategic sites, academia, and the arts, in short just about everything that makes Israel a viable state, are concentrated between Haifa and Ashkelon, in an area about 100 miles long and 10-15 miles wide. Further compounding its strategic vulnerability, Israel relies on a largely reservist army and therefore lacks the staying power required for protracted confrontations, which take an intolerable toll on its economy (see Maps 1 and 2).

Map 1


LEBANON
UNDOF Zone
Qiryat Shemona
SYRIA
Golan Heights
Nahariyya
Akko
Sea of Galilee
Haifa
Tiberias
Nazareth
MEDITERRANEAN SEA
Jordan
Hadera
Janin
Netanya
Tulkarm
Nablus
Herzliyya
West Bank
Tel Aviv-Yafo
1994 Treaty Line
Bat Yam
AMMAN
Ramla
Ramallah
Rehovot
Ashdod
Jericho
JERUSALEM
Ashqelon
Bethlehem
Qiryat Gat
Dead Sea
Gaza
Gaza Strip
Hebron
Khan Yunis
1950 Armistice Line
Beersheba
1949 Armistice Line
ISRAEL
Dimona
Zefa
Zin
Negev
JORDAN
Mizpe Ramon
EGYPT
Sinai
Yotvata
Elat
Gulf of Aqaba
0
40 km
0
40 mi

Map 2



Numerous states throughout history have faced a threat of politicide (destruction of the state). Israel is unique in that its leaders and people have always believed their country also faces a realistic threat of genocide and national extinction. From the beginning, Israel's leaders assumed that the conflict with the Arabs would last for decades or even centuries, and that the various wars and lower-level hostilities were just stages in one overall confrontation. To this day, some view the ongoing conflict with the Palestinians as a continuation of Israel's War of Independence in 1948. The dangers posed by Israel's external environment are thus considered to bear little substantive comparison to the dangers faced by other countries.[5]

The perpetual preoccupation with security gave rise to the preeminent role played by the defense establishment (the IDF and the intelligence agencies) in Israeli society. The IDF is not just another national military, whose sacrifices accord it the reverence common to militaries in many countries, but a unique embodiment of national rebirth and the guarantor of the nation's existence.

Much has changed in recent decades. A number of Arab states have made peace with Israel, and others have given up any practical intention to go to war against it. Indeed, the military conflict today is limited primarily to Iran and its nonstate actor allies, Hezbollah, Hamas, and others. Russia no longer constitutes a hostile superpower and Israel has a unique "special relationship" and strategic alliance with the United States.

Yet despite the overall improvement in Israel's strategic circumstances, it continues to view itself as a "nation dwelling alone" and to be driven by a fundamental sense of insecurity. The massacre of 1,200 Israelis in the Hamas attack of October 7, 2023, in which Israeli territory, towns, and villages were overrun for the first time since 1948, further reinforced this. The focus of Israel's strategic culture has thus been a never-ending quest for greater security, based the assumption that only Israel can bear ultimate responsibility for its defense and consequent strategic principle of self-reliance.[6]

Israel, it was long believed, could never match its adversaries' overwhelming quantitative economic, military, and diplomatic advantages. Instead, Israel would have to develop and maintain a qualitative advantage and, to this end, better mobilize its human resources. This meant the nearly universal military conscription of both men and women; better training, resourcefulness, and motivation for its military; and an emphasis on advanced technological capabilities.

Such capabilities, both civil and military, were considered strategic and economic imperatives from the state's earliest days. They were viewed as the keys to Israel's qualitative advantage and ability to be self-reliant, and have remained at the heart of Israel's national security strategy and socioeconomic policy ever since. Technological prowess was to function as the engine of Israel's socioeconomic development and, in turn, finance the defense burden, including domestically developed unique military capabilities.[7] This would require large-scale investment in education, science, and R&D. By the time the cyber realm emerged at the forefront of economics and security in the early 2000s, Israel had already become a leading international center of high-tech.

The cyber realm represented a new and potentially severe addition to the array of conventional, unconventional, and mostly asymmetric threats that Israel faced at the time. As such, its initial response was a matter of sheer strategic necessity. On the other hand, cyber appeared to be "made to measure" for Israel: it entails limited development and manufacturing costs; it requires only modest numbers of extremely talented and innovative scientific and technological personnel; and it has the potential for a relatively rapid and high return both economically and in the military domain. Israel thus viewed cyber not just as a strategic and socioeconomic imperative but as an opportunity.

Israel has used access to its cyber technology, and high-tech technology in general, as an inducement for foreign states to improve relations. The success of such "cyber diplomacy" was clearly demonstrated by the decision by the Abraham Accords states (UAE, Bahrain, and Morocco) to establish diplomatic relations with Israel and by the expanding informal ties with Saudi Arabia and other countries.[8]

Cyber is not just a blessing for Israel, however, but also the source of potential new vulnerabilities. Israel is far more cyber-dependent than its adversaries and therefore more vulnerable to attack. Indeed, Israel faces a nearly constant barrage of cyber-attacks originating from state and non-state actors alike, and such attacks have come to be viewed as one of the primary threats Israel faces today. In early 2023 alone, Israel blocked more than 1,000 attacks that had the potential to cause significant economic disruption. Over one-third of Israeli companies face at least one cyberattack every week.[9]

Practically every type of computer system that exists in Israel has been attacked. Critical infrastructure firms (electricity, water, communications) have been a particular focus of attacks, as have military targets. Other targets have included hospitals, airlines and airports, the Tel Aviv Stock Exchange, the Bank of Israel, media outlets, universities, the Home Front Command's rocket early warning system, government ministries and municipalities, and private firms of every variety including defense industries, as well as defense officials and even nuclear scientists. Hackers have successfully installed malware on IDF soldiers' cell phones that enabled them to listen in on their conversations and operational briefings and film their surroundings, including military bases and formations.[10]

Cyber-attacks against Israel have ranged widely in terms of the type and extent of the damage intended and levels of sophistication. Some have been for purposes of disruption, others for espionage, and still others for influence operations designed to inflame domestic divides, sow discord, and possibly affect electoral outcomes.[11] Some have been a combination thereof.

A number of examples of significant attacks illustrate the range of dangers cyber poses to Israel. Every year, on the eve of Yom HaShoah (Holocaust Remembrance Day), “hacktivist” groups conduct a coordinated series of cyber-attacks on Israeli websites. One such group has repeatedly threatened Israel with an “electronic Holocaust” and with being “erased” from cyberspace.[12] In 2019, foreign hackers almost succeeded in inserting fake video footage purporting to show rockets raining down on Tel Aviv into the televised broadcast of the Eurovision Song Contest, an annual European musical extravaganza held that year in Israel and viewed live by hundreds of millions of people. In 2020, hackers from Iran, China, North Korea, Russia, and Poland launched more than 800 cyber-attacks against Ben-Gurion Airport and approaching aircraft in the hope of disrupting the arrival of more than 60 world leaders attending a commemoration of the 75th anniversary of the liberation of Auschwitz. The list of dignitaries included the presidents of Russia and France and the vice president of the United States. In 2022, at the height of the war with Russia, hackers sought to disrupt President Zelinsky’s live address to the Knesset.[13] Had these attacks succeeded, the damage to Israel’s image and economy would have been severe.

Israel faces myriad military threats, and its largely reservist military has exceedingly short mobilization times. A cyber-attack that successfully disrupted power, communications, or transportation systems, even for a short period, could make a critical difference in times of war. Even something as basic as shutting off traffic lights or disrupting cellular communications could delay the mobilization of forces and have a significant impact on military operations, in addition to causing chaos throughout the country.

The intensity of cyber operations against Israel has been shown to increase significantly during periods of both military tensions and heightened diplomatic activity. Each year, the IDF and the intelligence community face countless attempts to break through their defenses and penetrate computer systems and networks, including operational ones.[14] Attacks that successfully penetrate command-and-control and intelligence systems, or even weapons systems, could potentially cripple critical military capabilities. Another major concern is the danger that a cyber-attack could escalate and lead to a kinetic military confrontation.[15] Overall, the most serious threat comes from Iran, but Hezbollah and Hamas are very active in the cyber realm as well.

Most known attacks against civilian targets thus far were designed to cause disruption, hardship, and damage to Israel's image and economy, and to compel Israel to change some of its policies. While a limited number of successful cyber-attacks at this level are unlikely to achieve these objectives, the constant bombardment does contribute to the long-term effort to wear Israel down. As in other forms of asymmetric conflict, Israel's adversaries do not seek to cause one or a few catastrophic cyber events but to wage a long-term campaign to undermine the resilience of Israeli society. In other words, death by a thousand cuts.

Part II: How Israel Became a Cyber Power

Five primary factors account for Israel's cyber prowess, all of which are closely tied to the unique role of the Israel Defense Forces (IDF) and intelligence agencies in Israeli life. They enjoy a symbiotic relationship with Israel's commercial cyber sector, academia, and government ministries, and their numbers and talent are fed by compulsory military service. The IDF and intelligence agencies make a singular contribution to the training and professional development of Israel's cyber experts, to Israeli cyber education in general, and to the country's unique national culture – what we call "chutzpah gone viral." Social networks are a further contributing factor.

Independent Variable I: The Symbiotic Relationship Between the Defense Establishment and the Commercial Cyber Sector, Academia, and Government Ministries

The importance of the defense establishment for the remarkable growth of Israel's high-tech sector generally, and cyber specifically, cannot be overstated. It was the defense establishment that first grew interested in cyberspace back in the 1990s, a consequence of the changes taking place in Israel's strategic landscape at the time, with a growing focus on asymmetric threats. The defense establishment was able to impress on the political leadership the importance of cyberspace for Israel's military as well as economic needs and to provide the necessary knowledge to help make the initial decisions.[16]

The decision to invest heavily in cyber began with a visit by Prime Minister Netanyahu to IDF Unit 8200.1 Netanyahu was deeply impressed and excited by what he heard and set out what has become the basic design for Israel's cyber strategy to this day. The government and IDF were to be responsible for defending both the civil and military cyber realms in industry and academia in order to develop Israel's cyber capabilities.[17] A specially convened task force submitted its recommendations shortly thereafter and Israel was on its way to cyber leadership.

The IDF, intelligence agencies, Air Force, and Ministry of Defense have been among the biggest driving forces of innovation in Israel.[18] All sponsor incubators and accelerators of cyber startups, providing knowledge, capital, and other resources to help develop capabilities with defense applications. In so doing, they have spawned countless commercial cyber products. A great many leading high-tech and cyber firms in Israel have been founded by veterans of high-tech IDF units, including Check Point, Palo Alto Networks, and NICE Systems.[19]

Intelligence Unit 81, the ultra-secret advanced technologies unit, demonstrates the impact of Israeli culture on the nation's success in cyberspace. The unit's motto is "turning the impossible into the possible" and it is at the forefront of global technology. Roughly 100 veterans of Unit 81 who served between 2003 and 2010 established 50 startups over the following decade with a total valuation of over $10 billion. One Unit 81 veteran who founded several highly successful startups explains this unusual entrepreneurial success rate this way: "A team that has worked together before is a substantial force multiplier. You can't find that in Silicon Valley, either in terms of the pool you can draw from, or in terms of knowledge and experience. Even Google and Microsoft don't have a concentration of talent like Unit 81."[20]

In 2019 the IDF, IAF, and Ministry of Defense established INNOFENSE, an innovation center designed to assist startups that develop commercial cyber with military applications. The Mossad similarly created a technology innovation fund called Libertad, which focuses on startups in a range of areas, including financial tech, robotics, AI, drones, remote personality analysis, voice analysis, synthetic biology, and blocking. The Mossad gains access to unique intellectual property, and the startups gain investments on attractive terms and retain commercial rights once the R&D stage has been completed.[21]

A key example of the symbiotic relationship between the different sectors of Israeli society is the Beersheba Advanced Technology Park (ATP), established in 2013. A joint venture of the government, local municipality, IDF, and Ben-Gurion University, the idea was to create a common space in which startups, multinational corporations, government agencies, academia, and the IDF would have offices. Proximity, it was hoped, would enhance opportunities for cooperation, increase the exchange of ideas, and enable each sector to assist the others, leading to greater innovation. As of 2023, over 70 companies have had offices in the ATP, including many global giants such as Lockheed Martin, IBM, Deutsche TeleKom, and Fujitsu.[22]

The IDF's new National Cyber Center, adjacent to the ATP, is nearing completion. The Center will house the C4I and Cyber Defense Branch's2 technological units and computer, cyber and communications schools, as well as Air Force and other units. The thousands of soldiers serving there will be able to register for courses at Ben-Gurion University. The IDF also plans to relocate various intelligence units, including Unit 8200, with a combined staff of approximately 19,000 people, to a new base near Beersheba.[23]

Independent Variable II: Compulsory Military Service

Compulsory military service is a primary source of Israel's high-tech prowess and at the heart of the unique Israeli nexus of the IDF, academia, and industry. Compulsory military service enables the IDF to harness the talents of Israel's best and brightest, essentially for free, for a period of years. In the cyber realm in particular, just a few geniuses play an outsized role and make all the difference. Many of the IDF's top talents were already employed by high tech firms prior to their induction at age 18. Their skills are in great demand among both multinational tech giants and Israeli firms, and many would not have served had they not been required to do so.[24]

Because of compulsory military service, the total talent pool available to Unit 8200 is unusually large, especially given Israel's diminutive size. Whereas the American National Security Agency (NSA) has approximately 40,000 personnel, Unit 8200 reportedly has as many as 10,000 – significantly smaller, but not by orders of magnitude.[25] Each year, between a few hundred and approximately 1,000 top-notch cyber experts, the very best Israel has, are discharged from the IDF and join the ranks of Israeli industry and academia. The 2022 graduating class of China's National Cyber Security School, by comparison, had about 1,300 students. Bottom line: compulsory service provides Israel with a cyber force on a scale nearly comparable to that of a global power.[26]

To find the very best and brightest, the IDF scours Israel's high schools and conducts intensive screening processes for the different units.[27] In practice, the IDF has a surplus of recruits who wish to serve in cyber units, including many who already have university degrees or work experience in leading tech firms. The competition for these recruits among IDF units is fierce, with first pick going to Military Intelligence.[28]

According to a former head of Unit 8200, now a high-tech entrepreneur: "The biggest secret of the Israeli high-tech system is the military's ability to look at people while they are (still) in high school." When combined with the hands-on experience gained through military service, as well as Israel's cyber capabilities in academia and high-tech firms, the result "sparks magic", in his view.[29] A former deputy head of 8200 puts it in similar terms: “The greatest present that we have is the high-quality personnel who get here every year. It is their inexperience and rapid turnover that contribute to rapid changes and rapid responses to changes in the environment. They grow up with a technology that is changing all the time. They are less rigid and, in many cases, change comes from below.”[30]

Independent Variable III: The Defense Establishment’s Contribution to the Training and Professional Development of Israel’s Cyber Experts and Leaders

The IDF’s critical need for highly trained and innovative personnel has made it one of the driving forces behind cyber education in Israel. In addition to supporting educational programs in the public school system, a variety of IDF units provide training programs that cover most areas of computer science, including mathematics, programming, infrastructure and network administration, software testing, and more. Overall, about 10,000 soldiers a year participate in these programs,[31] an indication of their subsequent impact on Israel’s high-tech sector generally.

One IDF program, Talpiot, seeks out the top 2% of high school students each year. Only 10% of them pass the initial battery of tests, mostly in physics and mathematics. This select group is then further winnowed down through grueling personality and aptitude testing. Those accepted to the program serve in the IDF for at least nine years, during which time they pursue undergraduate and graduate degrees, undergo specialized military training, and are typically involved in major R&D projects, many of critical importance for Israel’s cyber capabilities. The program has been highly successful by any metric. Approximately one-third of Talpiot participants choose to stay on in the IDF and pursue military careers, another third become academics, and many of the rest have gone on to become Israel’s most successful high-tech entrepreneurs.[32]

An offshoot of Talpiot, Odem, was jointly launched in 2022 by the IDF, Mossad, and the Israel Security Agency (ISA, otherwise known as Shin Bet) in conjunction with the Ministries of Defense and Education. The 12-year program begins in 10th grade with three years at a boarding school, followed by an undergraduate degree in electrical engineering at the Technion and six years of service in the IDF, Mossad, or ISA technological units. The program attracts participants by offering a free and personally tailored course of studies, a large support staff, and the assurance that graduates will have “enormous influence” during their military service.[33]

Unit 81’s selection process is nearly as grueling as Unit 8200’s. Some 10,000 people meet the initial criteria each year and several thousand reach the screening process, but only a few hundred end up serving in Unit 81 or similar units.[34] The Academic Reserves (akin to the American ROTC program) is still another source of exceptional personnel. Approximately 1% of high school graduates are given the opportunity to pursue undergraduate degrees in computer science, mathematics, engineering, and other areas of importance to the IDF prior to their compulsory service. In exchange, they are required to serve for an extended period, typically five years.[35]

Approximately 500-600 soldiers are trained each year in offensive cyber operations at the Ashalim school in Beersheba. Courses typically last 20 weeks and provide soldiers with the specific skill sets they will need in their future units. Between 25-30% of the trainees at Ashalim are graduates of Magshimim, a special cyber education program for underprivileged students (see below). The trainees are 12.5% women, a figure that has grown over time. In an effort to encourage women, who have been found to perform better in less competitive learning environments, trainees at Ashalim are not allowed to compare their achievements with each other but only with their own past performance.[36]

A “cyber defenders” course trains soldiers in how to detect and prevent attacks against military computers and networks.[37] In another course, soldiers are trained on a model Sim City, complete with residential and commercial neighborhoods, railways and airports, a nuclear ʳeactor, an electrical grid, a stock market, a military base, and a missile defense system, all of which must be protected. Trainees face simulated cyberattacks in which they learn to react quickly to protect the targets and are confronted with the consequences when they fail.[38]

One particularly innovative course is run by Intelligence Unit 9900, which is responsible for geospatial intelligence, including satellite and high-altitude surveillance images. This course trains autistic soldiers to do the highly exacting work of image interpretation, a skill at which they have proven particularly adept. The program's success led to the establishment of a cyber security training course for autistic soldiers. A number of private firms provide professional mentors to trainees and offer internships to graduates, potentially leading to long-term employment.[39]

IDF cyber training programs span the entire length of a soldier's compulsory service and beyond. A highly select group participates each year in intensive pre-induction cyber courses. Many participants then serve in the IDF's leading intelligence and technological units. Prior to discharge, combat soldiers are offered the opportunity to participate in seven-week cyber immersion courses that are designed to provide them with the skills needed for employment in the commercial cyber sector. Another program, Maagalim ("Cycles"), provides pre-discharge combat soldiers with an even more intensive training course in Unit 8200. At the end of the program, graduates can choose either to stay on in Unit 8200 or the C4I Branch for two years as paid professional personnel or join the commercial sector.[40]

Another way military service contributes to Israel's high-tech prowess by providing unusual professional experience and command responsibility to soldiers at a very young age. At a time when many of their peers abroad are still enjoying their final years of youth at college, these young soldiers are gaining real-world leadership experience, commanding technological or combat units, and/or learning advanced professional skills. It is an intense, transformative, and maturing experience. The result is a workforce with an extraordinary number of highly trained, motivated, and disciplined young people who have a pragmatic approach to problem-solving.[41]

A large part of Israel's success in cyberspace is the IDF's organizational culture, which is reflective of Israel's broader national culture. Much like other militaries around the world, the IDF is highly mission-focused. Unusually, however, the IDF encourages soldiers at all levels to think creatively rather than remain bound by structure and command from above. Officers are expected to express their views forcefully when they disagree or think something can be done more effectively, right up until the final decision is made, and to take the initiative and improvise to get things done. This approach entails a high command tolerance for dispute, rule-breaking, and risk-taking (within reason), so long as the objective is achieved.[42]

Part of the IDF's approach is to change the way recruits think. According to a senior cyber official, IDF training stresses the need "not to be afraid, to try, take risks, experience failure." A former commander of the "cyber defenders" course says soldiers are taught "to think differently, to search for things that are less visible, in the places where one does not usually look…that people have tried really hard to hide."[43] A former commander of Unit 81 described its recruitment and training programs in similar terms:

> When the soldiers are recruited the emphasis is not necessarily on their knowledge of computers or electronics. We are looking for people who can think outside the box, but who can also collaborate with others who have similar traits...We don't ask candidates to write code; instead we give them a complex problem to solve in order to examine how they come up with a solution.[44]

The organizational culture in Unit 8200 has been described as resembling that of a startup in that soldiers are encouraged to work "outside the box" and challenge authority. Unit 81 reportedly takes this even further. Unit 81 veterans often speak of the sense of freedom they enjoyed during their service, when little importance was attributed to rank and much more to expertise and charisma. Unit 81's assignments typically appear impossible to solve, but according to veterans, their experience learning to solve such problems partly explains their later success in the private sector.[45]

These units also instill a powerful sense of group cohesion. Veterans express a strong desire to continue working together after they have been discharged, and it is common for successful startups to be established and staffed by them. Another benefit, according to a former commander of Unit 81, is that conscripts "see veterans doing well and don't want to become salaried developers, but to blaze new paths, because that was the drive that was instilled in them."[46] Units 8200 and 81 may be unusual, but they do reflect something unique about the IDF in general, and they have a direct impact on Israel's civil high-tech sector.

To retain high quality cyber personnel despite the temptations of the private sector, the IDF has been forced to devise special models of military service for them. One such model, known as "industrial capsules", enables cyber personnel to work at private firms for given periods of time and then return to military service. Another model allows IDF cyber personnel to work for the IDF part-time while going to university or working for private firms.[47] In addition to generating improved retention rates (the primary objective), these models provide the IDF with the benefit of the experience gained by personnel working in the private sector. That sector, which suffers from a perpetual shortage of highly trained cyber personnel, also benefits.

Independent Variable IV: Cyber Education and Research

A limited supply of highly trained technological personnel has long been a primary obstacle to the expansion of Israel's cyber capabilities. While the IDF has had training programs of its own in place from the beginning, those programs have not been sufficient to meet its own needs, let alone those of the private sector. A focus on education has thus been key to Israel's success in the cyber realm.

To this end, the Israel National Cyber Directorate (INCD) formulated a strategy to expand the overall national pool of technological personnel. The strategy was based on three key decisions. The first was that schools should provide cyber education programs to children as young as possible, as research showed that students who were exposed to such programs at an early age were more likely to remain in the field. The second was to reach out to parts of the population that were underrepresented in technological fields, including young people from disadvantaged areas, women, ultra-Orthodox Jews and Israeli Arabs.[48] The third was to involve the high-tech sector and academic institutions in primary school cyber education programs.

The Cyber Education Center (CEC) was established in 2016 to implement these and other programs. Today, the CEC oversees a range of cyber education programs, from sixth grade through high school, that are designed to prepare students for future positions at high-tech firms and in academia as well as in the IDF and intelligence agencies. Some of these programs are run jointly with IDF units.[49]

The CEC's programs have been highly successful at increasing the number of people who enroll in cyber studies at the university level and thereby improving the overall quality of Israel's cyber human resources. For instance, the Magshimim ("Dream Fulfillers") program, which provides university-level cyber education to underprivileged high school students who have exceptional coding and hacking skills, was so successful that it was expanded to middle school students as well. Roughly 30% of Unit 8200's cyber personnel graduated from the program, and they are highly sought after in the private sector following their military service.[50]

Each year, the Ministry of Education, CEC, and several multinational R&D centers in Israel cosponsor a "Coding Olympics" (dubbed "Skillz") designed to encourage students to study coding and learn more about the cyber realm. Unit 8200 hosts competitions in which students attempt to disrupt a fictional adversary's servers, providing the unit with an opportunity to scout for prospective recruits. Similarly, the Israeli branches of Microsoft, Google, and other leading tech firms conduct hackathons in which teams compete to find the best means of preventing and mitigating simulated attacks.[51]

Every university in Israel now offers courses in cybersecurity, and in 2018, for the first time, more students registered for engineering than for any other academic discipline. Together with students of computer science, mathematics, and statistics, they now account for approximately one-quarter of all university students. In 2022, the National Economic Council said the number of students in high-tech disciplines had increased by 50% over the previous five years and projected that the number would continue to grow.[52]

A range of adult cyber training programs, often centered on underrepresented populations, is also available. For instance, "She

Codes" seeks to increase the percentage of female programmers in the high-tech sector. "Adva" (Ripple) helps ultra-orthodox women obtain undergraduate degrees in computer science and mathematics.[53]

R&D has been a key component of Israel's cyber ecosystem from the beginning. To this end, the government has poured hundreds of millions of shekels into commercial cyber R&D, and the INCD has helped establish cyber centers at universities across the country. As a consequence, the number of academic cyber researchers increased from 30 in 2013 to 200 in 2019. Academic scholarships and research grants that focus on cyber subjects are offered, and incentives, funding and grants are provided to companies that engage in cyber R&D and entrepreneurship.[54]

Today there are approximately 400 multinational R&D centers in Israel, many involved in cyber, with more opening each year.[55] The list reads like a global *Who's Who* of the top firms in the field.

Independent Variable V: Israel's National Culture and Cyber – Chutzpah Gone Viral

Israeli society has a number of traits that are particularly well suited to success in the cyber realm and high-tech generally. Some draw on Jewish traditions and experiences while others are more uniquely Israeli.

Jewish tradition has long stressed the value of knowledge, education, and critical learning, including yeshiva education, where students are actively encouraged to dispute interpretations of the Torah and other religious texts. Millennia of persecution and discrimination at the hands of hostile foreign rulers further imbued the Jewish people with a skeptical view of rules and authority. Because of this background, Israeli society has a deeply ingrained inclination to challenge authority; reject accepted norms, practices, and wisdom; refuse to take no for an answer; and search for alternative solutions.[56]

The propensity to challenge authority is further strengthened by the heterogeneous nature of Israeli society. Israel's population consists of immigrants from over 70 national and cultural backgrounds. Jews of Iraqi, Polish, Ethiopian, Russian, or American heritage, for example, share little in the way of a common social and cultural background.[57]

Further, roughly 20% of Israel's population is Muslim. Each of these groups has its own values, histories, experiences, and ways of doing things. The result is a constant state of social and cultural tension, but also an extraordinary degree of creativity.

Israel is an immigrant society. By their very nature, immigrants tend to be risk-takers and entrepreneurs, and consequently drivers of scientific and technological innovation. They also bring their own skills and knowledge to their new national homes and in so doing often raise local standards. In Israel's case, immigrants were forced to overcome not just the challenges of adapting to a new society but also the adversities faced by a rapidly developing state embroiled in a decades-long battle to assure its security and survival. Everyone had to be creative and seek innovative solutions.[58]

Adversity, at both the individual and national levels, is also a key driver of innovation. Faced with constant threats to its security and even survival, Israel has had to find creative ways to meet those challenges. This was especially true in the early years, when resources were scarce, institutions new and limited, and the conflict with Arab states most intense. Moreover, Israel's external and internal environments have always been characterized by a frenetic pace of change. These circumstances have imbued Israeli society with a marked ability to embrace and cope with change, an unusual propensity for improvisation, and a national decision-making style geared towards flexible responses to rapidly changing developments. What began as a necessary response to Israel's circumstances has remained a primary characteristic of Israeli decision-making to this day, in both the governmental and private sectors.[59] In a field like cyber, in which the pace of change and development is extraordinarily swift, these are highly valuable societal attributes.

A further characteristic of Israeli society is its unusually non-hierarchal and informal nature. The egalitarian norms established by the founders, best embodied in the early years by the kibbutz, remain characteristic of Israel to this day. In academic terms, Israel is considered a "small power distance society" in which formal hierarchy is paid little heed. The comparatively freewheeling and unregimented nature of Israeli childhood, along with parents' greater tolerance for risk in child-rearing, may contribute to this. Israeli children are generally allowed to experiment and take chances with relatively few constraints and social strictures.[60] No less important, Israeli culture combines two seemingly conflicting traits: a strong sense of individualism and a well-developed group orientation and willingness to act in pursuit of collective goals.[61] In part because of this and in part because of Israel's strategic circumstances, the government, private sector and defense sector manifest a greater willingness to work together in close collaboration than is found in most other democracies.

The above cultural attributes are highly characteristic of the business culture typically found in R&D and high-tech firms worldwide. They are key to success in the cyber realm.

Social Networks

Social networks are a further contributing factor to Israel's success in the cyber area. They can often provide critical information about scientific and technological developments, as well as business and employment opportunities, more efficiently than can markets or governments. Social networks are especially important in regard to geographically removed business and employment opportunities – of particular value for Israel, given its distance from international markets.[62]

Clusters are a particularly effective form of social network. Although Israel has several easily identifiable high-tech clusters, the physical distances between them are not great. Indeed, the territory of Israel between Haifa and Beersheba really constitutes a single "Silicon Wadi." The result is a readily accessible wealth of expertise and ease of communications that greatly facilitates R&D processes. The expert one needs, even national decision-makers, are usually no further than one or two degrees of separation away.

Nearly everyone in Israel's high-tech sector has served in the IDF, many in technological or combat units, further reducing social distance and facilitating development of close ties with the government, defense establishment, academia, and others in the private sector. Subsequent service in the reserves further bolsters and simplifies these connections.[63] Reservists gain firsthand exposure to the IDF's operational needs and can thus propose ideas for new or improved capabilities, matching IDF needs to the capabilities of the private sector. Many reservists also have close ties to senior business and governmental decision-makers, which greatly reduces the time that must elapse between the identification of a need and development of the necessary response.[64]

Ties with peers, former commanders, and fellow reservists help create a highly developed networking system for business, employment opportunities, and social connections. A single individual's military service can yield hundreds of ties at various levels.[65] Some headhunting firms specialize exclusively in veterans of IDF technological units. Units 8200, 81 and 9900 have veterans' associations with thousands of members. These associations host networking events to help members find employment in the R&D sector and promote business opportunities.[66]

Furthermore, veterans of these units tend to recruit their former subordinates and teammates when launching startups. A cycle is created in which the new recruits eventually leave those firms to found startups of their own, where they recruit new people who were discharged more recently from military service. Indeed, it is not rare for firms to be founded by teams comprised entirely of veterans from a single unit. Nor do the networking benefits end with the founding of firms or the recruitment and mentoring of newly discharged comrades. Younger veterans commonly raise capital from their predecessors in an informal angel circuit.[67]

Diasporas are a particularly efficient form of social network for connecting people and exchanging information and knowledge. Israel has therefore focused on building such networks to link Jewish communities, businesspeople, and financiers in the United States with startups and companies in Israel.[68] Similar efforts have taken place in other states as well.

Part 3: Conclusions

Cyber has at least partially upended the regional balance of power in the Middle East, providing Israel with important economic and military advantages. No other Middle Eastern state has a digital economy and cyber ecosystem as advanced as Israel's; nor have they applied cyber technologies for military purposes to the extent that Israel has.

Cyber has had important effects on Israel's regional and international standing. Israel has successfully leveraged cyber as a means of establishing and strengthening ties with a variety of states around the world via the aforementioned Abraham Accords and the expansion of informal relations with Saudi Arabia and other Arab states, as well as other countries of critical importance for Israel.

Cyber has contributed significantly to the ongoing socioeconomic and political turmoil that has continued to erupt in the Middle East ever since the "Arab Spring" of 2011. For reasons that go far beyond cyber but that are greatly facilitated by it, this regional turmoil is likely to continue for decades, with significant ramifications for Israel's security. To the extent that Israel's adversaries are weakened militarily by the turmoil, the impact on its national security will be positive. If, however, those adversaries' internal instability spills over their borders, the impact on Israel will be highly deleterious.

Cyber information operations have provided Israel's adversaries with a host of new platforms on which to reach vast numbers of people around the world, instantly and at minimal cost, as part of their ongoing efforts to delegitimize Israel and isolate it diplomatically. They have also provided them with powerful means of creating international pressure on Israel to halt, or at least curtail, military operations before they have had time to achieve their objectives. Cyber information operations have thus had an adverse effect on Israel's ability to wage war and on its international standing. This has been demonstrated repeatedly in recent years, but was particularly pronounced during the 2023-2024 war in Gaza.

Israel's offensive and defensive cyber capabilities have become important components of its military might, as have its cyber-based intelligence capabilities. In a world increasingly averse to human losses and in which Israel is repeatedly excoriated for allegedly disproportionate uses of force, cyber provides an important means of achieving at least some military objectives without loss of life and property and with reduced risks of retaliation and escalation.

At the same time, Israel's vibrant cyber ecosystem constitutes a significant portion of its GDP today and is a primary engine of economic growth. The Israeli cyber ecosystem is in many ways unparalleled, producing world-class cyber talent not just in quality but in absolute numbers, on a par with the major powers. Conversely, Israel's greater cyber dependency, both civil and military, than that of its adversaries is a significant vulnerability, as it provides those adversaries with opportunities to cause it harm.

Despite Israel's successes, there are troubling signs on the horizon. One major issue is the decades-long, and still continuing, deterioration of Israel's educational system.[69] A second is a worrisome decrease in government funding for academic R&D. Together, these trends endanger Israel's leading international role in innovation and high-tech. If Israel cannot provide high-quality personnel, multinational companies will go elsewhere. Uncertainty and risks associated with the 2023 "judicial reform" efforts have also taken a toll, with roughly 70% of startups polled saying they have taken steps to move resources, employees, and even headquarters out of Israel as a result; some firms have reported layoffs as well.[70] This trend has been further exacerbated by the war in Gaza. The "NSO scandal", an international backlash against sales of offensive cyber weapons by Israeli firms to authoritarian regimes, also harmed Israel's image and may have led to an overly strong counterreaction against it that essentially put an end to its offensive cyber export industry.

More positively, Israel is investing in new technologies in high priority areas, including artificial intelligence (AI), 5G, digital medicine, and more. In the meantime, Israel's cyber ecosystem continues to be a singular source of innovative creativity.

Israel's success in cyberspace has been a remarkable story. In fact, one would be hard-pressed to think of any other area in recent decades in which Israel has prepared for an emerging threat and opportunity as rapidly, effectively, and successfully as it has in the cyber realm. We have argued that Israel owes this success to a number of factors, including the unique contribution of the defense establishment to Israeli life, an emphasis on education, and a unique national culture.

Bibliography

Adamsky, D. *The Culture of Military Innovation.* Stanford: Stanford Press, 2010.

Adamsky, D. "Israeli Culture of Innovation Between Anticipation and Adaptation". *Bein Haktavim*, Dado Center, IDF, July 2019.

Adamsky, D. "The Israeli Odyssey Toward its National Cyber Security Strategy." *The Washington Quarterly* 40 No. 2 (2017), pp. 113-127.

Arieli, I. *Chutzpah: Why Israel's a Hub of Innovation and Entrepreneurship.* New York: Harper, 2019.

Baram, G. and Ben-Israel, I. "The Academic Reserve: Israel's Fast Track to High-Tech Success", *Israel Studies Review* 34 No. 2 (November 2018), pp. 75-91.

Ben-Israel, I. *Israel Defense Doctrine* (Hebrew), Modan: Ben Shemen, 2013.

Brun, I. "Where Did Maneuver Disappear To? (Hebrew)." *Maarachot*, 420, no. 421 (September 2008), pp. 4-15.

Cohen, M.S., Freilich, C.D., and Siboni, G. "Israel and Cyberspace: Unique Threat and Response", *International Studies Perspectives* 17 No. 3 (August 2016), pp. 307-321.

Cohen, M. S., Freilich, C. D., and Siboni, G. *Israel and the Cyber Threat: How the Start-Up Nation Became a Global Cyber Power.* Oxford: Oxford University Press, 2023.

Dror, Y. *Israeli Statecraft: National Security Challenges and Responses.* London: Routledge, 2011.

Even, S. and Siman-Tov, D. "Cyber Warfare: Concepts and Strategic Trends." *Memorandum No. 117.* Institute for National Security Studies (2012).

Frei, J., *Israel's National Cyber Security and Cyber Defense Posture: Policy and Organizations*. Zürich: Center for Security Studies (September 2020).

Freilich, C.D. *Zion's Dilemmas: How Israel Makes National Security Policy*. Ithaca: Cornell Press (2012).

International Institute for Strategic Studies (IISS). "Cyber Capabilities and National Power: A Net Assessment." *Research Papers*. (June 28, 2021).

Israel Innovation Authority. "State of Innovation in Israel 2021" (2021).

Kahane, B. "Tikun Olam": How a Jewish Ethos Tries Innovation, *Journal of Management Development* 31 No. 9 (2012), pp. 938-946.

Matania, E. and Rappaport, A. *Cybermania: How Israel Became a Global Force in the Realm That Is Shaping the Future of Humanity* (Hebrew). Kinneret, Zmora, Dvir, Israel (2021). (In Hebrew; also available in English.)

Rid, T. *Cyber War Will Not Take Place.* London: C. Hurst and Co. (2013).

Senor, S. and Singer, S. *Start-Up Nation*. New York: Hachette Book Group (2009).

Swed, O. and Butler, J.S. "Military Capital in the Israeli Hi-Tech Industry." *Armed Forces in Society* 41, No. 1 (2013), pp. 123-141.

Tabansky, L. "Israel Defense Forces and National Cyber Defense." *Connections: The Quarterly Journal* 19, No. 1 (2020), pp. 45-62.

Tabatabai, A.M. "Iran's Authoritarian Playbook: The Tactics, Doctrine and Objectives Behind Iran's Influence Operations". *Alliance for Securing Democracy* (2020).

Taylor, M.Z., *The Politics of Innovation: Why Some Countries Are Better Than Others at Science and Technolog*y. Oxford: Oxford University Press (2016).

Yaniv, A. *Deterrence Without the Bomb: The Politics of Israeli Strategy*. Lexington, MA: D.C. Heath and Company, 1987.

References

In order to enable the officials interviewed for this study, current and former, to speak freely, they were assured of confidentiality and are usually referred to in the footnotes by an assigned number rather than by name. The interviewees spoke with the clear understanding that they were doing so in their individual capacities and expressing their personal views, not official positions. The conclusions presented are the authors' alone and do not reflect either official positions or those of the interviewees.

Notes

[1] International Institute for Strategic Studies 2021.

[2] http://nocamels.com/2017/01/bloomberg-innovation-index-israel-tenth/; http://www3.weforum.org/docs/GCR2016-2017/05FullReport/TheGlobalCompetitivenessReport2016-2017_FINAL.pdf.

[3] Adamsky 2010, p. 6; Adamsky 2019, pp. 1-2.

[4] http://www.pitgam.net/data/%5B%D7%9E%D7%A0%D7%97%D7%9D+%D7%91%D7%92%D7%99%D7%9F%5D/1/1/0/; Peter Hirschberg, Haaretz, 11/14/06.

[5] Yaniv 1987, pp.18-19; Ben-Israel 2013, pp. 59-60; Freilich, 2012, p.12; Dror 2011, pp. 13,16; Brun 2008, pp. 4-15.

[6] Freilich 2012 and 2018; Adamsky 2010, pp. 113, 115; Tal 1996, pp. 62–63; Levite 1989, p. 35; Feldman and Toukan 1997, p. 8.

[7] Taylor 2016. 143-144, 220, 229-230; Adamsky 2010. 113-114, 126; Baram and Ben-Israel 2018.

[8] https://www.timesofisrael.com/report-israeli-spyware-helping-dictatorships-track-dissidents-minorities/;https://www.reuters.com/article/us-israel-hackers/israel-eases-rules-on-cyber-weapons-exports-despite-criticism-idUSKCN1VC0XQ.

9 https://www.jns.org/israel-blocked-more-than-1000-cyber-attacks-in-2022/; https://www.calcalistech.com/ctech/articles/0,7340,L-3920707,00.html

10 *Times of Israel*, January 30, 2018; Morgan Dombowshi, *IronNet*, September 15, 2021; Yuval Mann, *YNet*, November 10, 2021; Rid 2013, p. 103; Tal Shahaf, *Ynet*, May 8, 2019; Yoav Zitun, *YNetnews.com*, January 11, 2017; Yoav Zitu, *YNet*, July 14, 2019.

11 Ben Caspit, *Al-Monitor*, February 12, 2019; Yonah Jeremy Taub, *Jerusalem Post*, February 25, 2019; David Horovitz, *Times of Israel*, February 6, 2019; Bergman, *Ynet*, July 31, 2018; Netael Bendel, *Haaretz*, December 7, 2020; Tom Bateman, *BBC*, February 3, 2022; Tabatabai 2020, pp. 15-19.

12 James Vincent, *The Independent*, July 29, 2014; Hirshoga and Nati Toker, *The Marker*, November 22, 2012; Olga Khazan, *The Washington Post*, November 17, 2014; Michal Zippori, *CNN*, January 26, 2012; Nati Toker, *Tech Nation*, January 22, 2012; Stuart Winer, *Times of Israel*, August 17, 2014; Jack Moore, *Newsweek*, April 7, 2015; Stuart Winer, *Times of Israel*, April 7, 2015.

13 Fiona Willian, *9 News*, July 2, 2019; "Eurovision Song Contest – Statistics and Facts," *Statista*, September 16, 2019; Nor Dvori, *HaMadura HaMerkazi*, January 26, 2019; *Times of Israel* Staff, January 26, 2020; *Jerusalem Post* Staff, March 20, 2022.

14 Itam Elmadon, *N12,* January 21, 2021; Yoav Limor, *Israel Hayom*, February 7, 2019.

15 Jordan Brunner, *The Tower.com*, August 2015.

16 Adamsky 2017, p. 114; Baram 2017, p. 6; Tabansky and Ben-Israel 2015, pp. 31, 35.

17 Matania and Rappaport, *Cybermania*, 2021, pp, 35, 40.

18 Tabansky 2020; Taylor 2016.144; Omer Keilaf, *Forbes*, July 3, 2020.

19 Adamsky 2017, p. 123; Omer Keilaf, *Forbes*, July 3, 2020; Swed and Butler 2013; https://www.wsj.com/articles/israeli-army-builds-

a-desert-outposttech-firms-follow-1433525715; https://www.forbes.com/sites/elizabethmacbride/2016/07/18/five-lessons-on-cybersecurity-from-an-israeli-general/#616d36a74fd1.

20 Sophie Shulman, *Calcalist*, January 8, 2021; https://81amit.org.il/about/.

21 Shoshana Solomon, *Times of Israel*, May 22, 2019.

22 http://www.readitnow.co.il/news; Richet 2015, 293; Ellen Nakashima and Ruth Eglash, *Washington Post*, May 14, 2016; Erad Atzmon Shmayer and Amitai Ziv, *The Marker*, July 11, 2019; https://www.gavyam-negev.co.il/en/about-the-park/

23 http://www.mod.gov.il/Society_Economy/articles/Pages/10.2.16.aspx; Viva Sarah Press, *Israel21c.org,* August 3, 2015.

24 Interviews with senior official #1, #2 and #14 and Tom Ahi Dror; IISS 2021.

25 Interview with senior official #1; Frei 2020.

26 Dakota Cary, *Defense One*, July 23, 2021;https://www.mako.co.il/news-military/2021_q3/Article-b861796623d7b71026.htm?utm_source=AndroidNews12&utm_medium=Share; Interview, senior official 2.

27 Inbal Orpaz, *Haaretz*, April 18, 2014; Christa Case Bryant, *Christian Science Monitor,* June 9, 2013; Amos Harel, *Haaretz,* November 14, 2013; Ellen Nakashima and William Booth, *Washington Post*, May 14, 2016.

28 Amos Harel, *Haaretz*, October 4, 2017.

29 Ellen Nakashima and William Booth, *Washington Post*, May 14, 2016.

30 Amos Harel, *Haaretz*, September 25, 2022.

31 Christa Case Bryant, *Christian Science Monitor*, June 9, 2013; Cohen, Freilich and Siboni 2015, p. 5; Inbal Orpaz, *Haaretz,* May 19, 2015.

32 Senor and Singer 2009, pp. 70-72; Baram and Ben-Israel 2018; https://bit.ly/3LrOgBm

33 Or Kashti, *Haaretz*, January 16, 2022.

34 Sophie Shulman, *Calcalist*, January 8, 2021.

35 Baram and Ben-Israel 2018.

36 Amitai Ziv, *Haaretz Weekend Magazine in English*, May 30, 2019.

37 http://www.haaretz.com/israel-news/second-group-of-cyberdefenders-graduate-from-idf.premium-1.492778; http://zahal.com/2015/09/idfs-cyberdefenders-complete-training-course/

38 https://www.idfblog.com/2017/01/02/model-city-trains-coders-stop-hacks/; https://www.ynetnews.com/articles/0,7340,L-4683636,00.html

39 Amir Mizroch, *Forbes*, May 28, 2018; Shoshana Solomon, *Times of Israel*, July 22, 2019.

40 Sophie Shulman, *Calcalist*, January 8, 2021; Yossi Yehoshua, *YNet*, February 15, 2022; https://www.timesofisrael.com/idf-teaches-combat-soldiers-cyber-skills-as-springboard-to-civilian-life/

41 Senor and Singer 2009, pp. 67, 74; Swed and Butler 2013; Omer Keilaf, *Forbes*, July 3, 2020.

42 Adamsky 2010, pp. 111, 117–118; Senor and Singer 2009, pp. 74, 98; Tabansky and Ben-Israel 2015, p. 20.

43 http://www.haaretz.com/israel-news/second-group-of-cyberdefenders-graduate-from-idf.premium-1.492778; Yonah Jeremy Bob, *Jerusalem Post*, December 10, 2020; Yaakov Katz, *Jerusalem Post*, May 31, 2012.

44 Sophie Shulman, *Calcalist*, January 8, 2021.

45 John Reed, *Financial Times*, July 10, 2015; Sophie Shulman, *Calcalist*, January 8, 2021.

46 Sophie Shulman, *Calcalist*, January 8, 2021.

47 Amitai Ziv, *The Marker*, October 1, 2017.

48 Interviews, Tom Ahi Dror and Sagy Bar.

49 Yossi Yehoshua, *YNet*, July 13, 2022; Interview, Tom Ahi Dror.; http://www.timesofisrael.com/in-israel-teaching-kids-cyber-skills-is-a-national-mission

50 Interview, Sagy Bar; Interview, Tom Ahi Dror; Yossi Yehoshua and Reuven Weiss, *YNet*, December 6, 2020; Frei 2020; www.csmonitor.com/World/Middle-East/2013/0609/Israel-accelerates-cybersecurity-know-how-as-early-as-10th-grade

51 Interview, Sagy Bar; Niv Ellis, *Jerusalem Post*, October 28, 2015, http://www.jpost.com/Business-and-Innovation/Health-and-Science/Multinationals-invest-in-teaching-Israeli-kids-to-code-430250; http://www.iati.co.il/news-item/1856/2016-national-coding-olympics-underway

http://cyberknight.co.il/;http://www.timesofisrael.com/in-israel-teaching-kids-cyber-skills-is-a-national-mission/;https://www.chaire-cyber.fr/IMG/pdf/tr_article_3_21_-_chaire_cyberdefenseeng.pdf

52 Nehemia Strassler, *Haaretz*, August 4, 2017; Stewart Winer, *Times of Israel*, January 16, 2017; Adir Yanko, *Ynet*, October 4, 2018; Meirav Arlozorov, *The Marker*, February 10, 2022.

53 Sivan Klingweil, *The Marker*, January 23, 2020; https://she-codes.org/about; Shoshana Solomon, *Times of Israel*, August 28, 2019; Corinne Degani, *The Marker*, August 8, 2021.

54 Matania and Rapppaport, Cybermania, 2021, pp. 375–387; Baram 2013, p. 34; Adamsky 2017, p. 118; Amitai Ziv, *The Marker*, July 15, 2019;

http://www.matimop.org.il/programs.html; http://economy.gov.il/English/Pages/default.aspx;http://economy.gov.il/English/About/Pages/About.aspx; http://www.pmo.gov.il/English/MediaCenter/Spokesman/Pages/spokekidma131112.aspx;https://innovationisrael.org.il/en/sites/default/files/2018-19_Innovation_Report.pdf;;

https://www.gov.il/he/departments/policies/2014_dec2092; https://rio.jrc.ec.europa.eu/en/library/rio-country-report-israel-2015;https://www.arnon.co.il/sites/default/files/files_from_old/Client%20Update%20-%20OCS%20-%20Amendment%207%20to%20R%26D%20Law%20%28YA-10.2015%29_0.pdf; https://www.rcip.co.il/en/article/on-the-establishment-of-a-national-authority-for-technological-innovation-amendments-to-the-law-for-the-promotion-of-industrial-research-and-development/; https://www.law.co.il/en/news/2016/01/05/israel-r-d-law-establishes-new-authority-for-innovation/; https://mof.gov.il/chiefecon/internationalconnections/oecd/oecd%20enterp.pdf.

55 Israel Innovation Authority 2021, p. 18; http://innovationisrael-en.mag.calltext.co.il/article/69/1141.

56 Tabansky and Ben-Israel 2015, pp. 18, 23; Baram and Ben-Israel 2018; Senor and Singer 2009, pp. 18, 51, 54; Kahane 2012, pp. 939, 942–945.

57 Senor and Singer 2009, p. 70.

58 Kahane 2012, p. 942; Omer Keilaf, *Forbes*, July 3, 2020.

59 Freilich 2012.33–34, 44, 71; Ellen Nakashima and William Booth, *Washington Post*, May 14, 2016.

60 Judy Rudoren and Isabel Kershner, *New York Times,* June 18, 2013; Adamsky 2017, pp. 110, 123; Arieli 2019, Chapter 5.

61 Adamsky 2010, p. 110.

62 Taylor 2016, pp. 142, 146, 158-160.

63 Swed and Butler 2013; Tabansky and Ben-Israel 2015, p. 20.

64 Even and Siman-Tov 2012.22; Institute for National Security Studies and the Cyber Security Forum Initiative. 2014a; Swed and Butler 2013.

65 Swed and Butler 2013.

66 John Reed, *Financial Times*, July 10, 2015; Tabansky and Ben

Israel 2015, 20; https://81amit.org.il/about/; https://www.9900.org.il/about

67 Sophie Shulman, *Calcalist*, January 8, 2021.

68 Kahane 2012.941; Taylor 2016, pp. 159, 166.

69 https://shoresh.institute/research-paper-eng-Ben-David-Kimhi-EducOverview.pdf.

70 cnn.com/2023/08/11/middleeast/israel-political-crisis-startups-mime-intl/index.html

Recent BESA Center Publications

Mideast Security and Policy Studies

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

No. 207 Could Israel's Nuclear Deterrent Support "Escalation Dominance" Against Iran?, *Louis René Beres*, September 2024

No. 208 Israel's National Security Concept: Insights from the Iron Swords War, *Eado Hecht,* September *2024* (Hebrew only)

No. 209 Israel: The Making of a Global Cyber Power, *Matthew S. Cohen and Charles (Chuck) D. Freilich,* October 2024

besacenter.org