Journal of Military and Strategic Studies

VOLUME 20, ISSUE 4

STUDENT AWARD OF EXCELLENCE 2021
FIRST PRIZE

The Theory, Pursuit, and Practice of Cyber power in Israel

Kyle McCreanor

> We realized […] early on that our small geographic size need not limit our cybersecurity capabilities. In fact, I think it's the opposite. I think because we are small, we have that power. We're small, we're concentrated, so there are a lot of fine young people, which means fine young brains that interact.
>
> Benjamin Netanyahu, Prime Minister of Israel (2017)[1]

Introduction

German sociologist Max Weber canonically described power as being in a position to execute one's will despite resistance.[2] Around the same time as Weber,

[1] Benjamin Netanyahu, "Prime Minister Benjamin Netanyahu's Remarks at the Cyber-Tech Conference," (speech, Tel Aviv, 31 January 2017), https://www.gov.il/en/departments/news/speechtech310117.
[2] Max Weber, *Economy and Society: An Outline of Interpretive Sociology*, eds. Guenther Roth and Claus Wittich (Berkeley: University of California Press, 1978) [1921], p. 53.

ISSN : 1488-559X

Italian general Giulio Douhet linked airpower to the capacity of a state "to be in a position to prevent the enemy from flying while retaining the ability to fly oneself."[3] Along these same intuitive lines British Rear-Admiral Philip Howard Colomb described *command of the sea* as the "power to prevent the passage of an enemy intending to descend upon the land."[4] That land, sea, or air power implies an ability to impose one's will in that domain is a truism to any student of military strategy. However, this understanding does not hold without problem in the nascent cyber domain. There is no unanimous agreement on what cyber space *is*, let alone how one ought to command it. Indeed, much of the classic language of strategy extended into cyber space has been criticized as inappropriate.[5] Nevertheless, that has not stopped states from developing strategies for *cyber warfare* or from trying to acquire *cyber power*.

Israel officially adopted the goal to become "one of the five leading cyber powers in the world" in 2011.[6] Prime Minister Benjamin Netanyahu said in 2017 that "I think by all accounts, we're there. But the jury in cyber security is always out. And it's a constant challenge."[7] There is wisdom in this musing, even though he contradicts himself—by what means is power measured here? Israel is well-known for its prowess in cyber warfare and its government has enthusiastically promoted this image.[8] Surrounded by hostile actors - Iran in particular with its willingness to conduct offensive cyber operations - the state of Israel has an obvious incentive to develop cyber power, or a capacity to competitively operate in cyber space. This paper takes Israel as a case study for how states have thought about the cyber domain strategically and how they have extended traditional concepts of strategy thereto. While classical military language may

[3] Giulio Douhet, *Command of the Air*, trans. Dino Ferrari (Alabama: Air University Press, 2019) [1921], p. 22.
[4] Philip Howard Colomb, *Naval Warfare, Its Ruling Principles and Practice Historically Treated* (London: W.H. Allen and Co. Ltd., 1891), p. 204.
[5] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic* Studies 35, no. 1 (2012): pp. 5-32.
[6] The Blavatnik Interdisciplinary Cyber Research Center, TAU, "Main Plenary – Prime Minister of Israel, Mr. Benjamin Netanyahu," YouTube video, 8:44, https://www.youtube.com/watch?v=QVh7uEWP4ik; Israel, Prime Minister's Office, Resolution no. 3611 "Promoting National Capacity in Cyberspace," 7 Aug. 2011, https://www.gov.il/he/departments/policies/2011_des3611.
[7] The Blavatnik Interdisciplinary Cyber Research Center, TAU, "Main Plenary – Prime Minister of Israel, Mr. Benjamin Netanyahu."
[8] Fabio Cristiano, "Israel: Cyber Defense and Security as National Trademarks of International Legitimacy," in *Routledge Companion to Global Cyber-Security Strategy*, eds. Scott Romaniuk and Mary Manjikian (New York: Routledge, 2020), pp. 409-417.

be adopted merely as a metaphor for the sake of familiarity, such patterned thinking can also guide practice consciously or unconsciously.[9] Problematically for this analysis, Netanyahu's aim to make or maintain Israel as a global cyber power rests on an expansive definition of cyber power with certain facets that this paper cannot explore. Rather than considering investment in the Israeli information technology (IT) industry, for example, we will concentrate on the aspects of cyber power more conducive to a military-strategic analysis: Israeli cyber-offence and cyber-defence as theorized and as practiced.

The Strategic Roots and Beginnings of Cyber Warfare in Israel

As in most other countries, the government of Israel was reactive rather than proactive in the 1990s about what we might term a *cyber policy*, which was left to individual departments and agencies. A state-sponsored commission recommended in 1989 that the government adopt a coherent approach to IT, but the slow gears of the policy world rarely deal well with emergent technologies.[10] Various government branches set up websites with the help of the private sector, but some of these were susceptible to hacking. The government established the civilian cyber security agency, *Tehila*, in 1997 to protect against cyber attack - understood herein to mean an operation that "uses and targets computers, networks, or other technologies for malevolent, destructive, or disruptive purposes."[11] (By extension we can consider cyber defence to be how an actor uses computers, networks, or other technologies to defend against such attacks.) Another means of securing the cyber domain from what is typically is the greatest vulnerability is improving simple information security practices by personnel. The Israeli government standardized its approach in 1999, developing a program to

[9] Miguel Alberto Gomez, "Overcoming Uncertainty in Cyberspace: Strategic Culture and Cognitive Schemas," *Defence Studies* 21, no. 1 (2021): pp. 25-46; Jordan Branch, "What's in a Name? Metaphors and Cybersecurity," *International Organization* 75 (2021): pp. 39-70.

[10] State Comptroller of Israel, "Using Information Technology to Provide Government Services to the Public," (April 2003): p. 2, https://www.mevaker.gov.il/he/Reports/Report_361/1e0d9521-0679-4b03-ad7d-11d546604a29/InformationTechnology_and_eGovernment53b.pdf.

[11] Matthew Cohen, Charles Friedlich, and Gabi Siboni, "Israel and Cyberspace: Unique Threat and Response," *International Studies Perspectives* 17 (2016): p. 309; There are countless definitions in the literature though this is among the better conceptualizations for our purposes as it does not limit the analysis to state actors as some other definitions do.

better screen and train employees in contact with computers, physically protect hardware, and implement biometric security.[12]

Israel did not publish a public defence strategy until 2015, forcing scholars to read strategy into practice prior to that point.[13] Isaac Ben-Israel, a chief Israeli cyber-strategist and a close confidant of Prime Minister Netanyahu, makes a number of important observations on what he deems to be the overarching *national grand strategy* that explains its approach. Above all, he writes, Israel has long prioritized "qualitative superiority to balance numerical inferiority."[14] In fact, we find this concept formalized in an Israel Defence Forces (IDF) document from 1953, which recommended using scientific superiority to "to create relatively secret weapons" not available to their enemies.[15] Israel's notoriously secret, the ambiguously-referenced nuclear arsenal, is one aspect of this strategy, described by Michael Handel as "the ultimate technological panacea."[16] Developing cyber power can be seen as another aspect of this strategy. Israel's longstanding attention to science and technology as a means of enhancing its strategic edge in the regional balance of power suggests that its government was predisposed to cyberwarfare.

Ben-Israel further identifies the traditional emphasis on deterrence as guiding Israeli cyberwarfare strategy. Historian Shmuel Bar traces the formal expression of the "doctrine of active defense and pre-emption" to the writings of Zionist leader Ze'ev Jabotinsky in the early 1920s. Israel's first Prime Minister David Ben-Gurion was well-versed in classical strategy (and the work of his political rival, Jabotinsky) and adopted the doctrine of *strategic deterrence*, understanding that Israel was too small and conventionally weak to take a permanently defensive posture.[17] The importance of this

[12] Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel* (New York: Springer, 2015), p. 32.
[13] Ibid., p. 4.
[14] Ibid., p. 11.
[15] Aniram Oren, Oren Barak, and Assaf Shapira, "'How the Mouse Got His Roar': The Shift to an 'Offensive-Defensive' Military Strategy in Israel in 1953 and Its Implications," *The International History Review* 35, no. 2 (2013): p. 362.
[16] Michael Handel, "The Evolution of Israeli Strategy: The Psychology of Insecurity and the Quest for Absolute Security," in *The Making of Strategy: Rulers, States, and War*, eds. Williamson Murray, Alvin Bernstein, and MacGregor Knox (Cambridge: Cambridge University Press, 1999), p. 551.
[17] Shmuel Bar, "Israeli Strategic Deterrence Doctrine and Practice," *Comparative Strategy* 39, no. 4 (2020): pp. 324-325.

idea in Israeli strategic thought is manifest in the state's early development and emphasis on cyber-offensive operations against its foes.

Israel was embroiled in some of the earliest cyber conflicts against state and non-state actors alike. The embattled state found itself at the centre of what has been called "the first full scale cyberspace war" during the Second Intifada (2000-2005).[18] Most of the so-called *Interfada* was waged between individuals and loose collectives in a fairly anarchic manner, with attribution being inherently hard to discern in the cyber domain. The Israeli cyber security regime was insufficient, as Palestinians were able to take down the websites of the Knesset (parliament), the Prime Minister's Office, the IDF, and the Bank of Israel. Israelis downed the website of Hezbollah for a few days, and the two sides engaged in back-and-forth takedowns and defacements of private sector websites.[19] A technological asymmetry worked against Israel in this case; there were more internet users there than in all Arab countries combined at the height of the Interfada in 2002. One Israeli hacker remarked that they had far more to lose because "the Israeli economy is based on internet companies."[20] E-Jihad, as its proponents called it, was wishfully seen as the tool of the oppressed that could severely harm the state of Israel through economic disruption.[21] This was relatively exciting to theorists in the early 2000s, with many journalists and academics offering views on the ostensibly new era of (cyber) warfare. In reality, Israel was not quite brought to its knees, and neither was Hezbollah, though this episode demonstrated what inconvenience could be effected with some knowledge, determination, and an internet connection at a cyber café.

The Israelis are thought to have begun working with the Americans on the notorious *Stuxnet* cyber weapon around 2007.[22] The destructive piece of code was utilized in a top-secret operation years in the making, blending human intelligence, cyber attack, and industrial sabotage. A nuclear facility in Natanz, Iran, was a high-value target to Israel according to its longstanding policy of employing preemptive

[18] Markku Jokisipilä, "E-Jihad, Cyberterrorism and Freedom of Speech," in *War, Virtual War and Society: The Challenge to Communities*, eds. Andrew Wilson and Mark Perry (Amsterdam: Brill, 2008), p. 92.
[19] Ibid., p. 103.
[20] Giles Trendle, "Cyberwars: The coming Arab E-Jihad," *The Middle East* (Apr. 2002), p. 7.
[21] Ibid., p. 6.
[22] Rid, "Cyber War Will Not Take Place," p. 17.

attacks to prevent its enemies from obtaining nuclear weapons (often called the *Begin Doctrine* by observers, after Prime Minister Menachem Begin).[23] Exactly as predicted by John Arquilla and David Ronfeldt in 1993, a cyber attack could be employed as a tool for counterproliferation.[24] The *Stuxnet* malware was injected somewhere inside the nuclear facility, probably by way of a USB drive inserted by an unsuspecting employee. Once connected, it subtly sabotaged vital gas centrifuges by reprogramming them to spin faster than they could handle. The malware then fed bogus data to the facility operators so as not to alert to them that parts were degrading.[25]

Stuxnet was eventually discovered in 2010 and the extent to which it retarded the Iranian nuclear program is uncertain. Much like the *Interfada* or *E-Jihad*, Stuxnet attracted much excitement and speculation. Michael Rid points to the declaration in *Vanity Fair* that it was "the Hiroshima of cyber-war" as among the worst exaggerations.[26] While there was much new about the kinetically destructive power of half a megabyte of code, the Stuxnet attack on Iranian nuclear enrichment is fairly conventional when viewed within broader Israeli strategy; it followed the Begin Doctrine, and also fit within the pattern of Israel's longstanding expertise in covert operations and industrial sabotage.[27] The Israelis thought it more classical still, sneaking in a line of code that hinted at the Book of Esther, in which the Jews preemptively strike the Persians who were plotting to exterminate them.[28]

Journalist David Sanger reports that the Americans brought Israel onto the project because of their technical expertise, intelligence on the facility, and to provide them an alternative to a conventional attack (i.e. airstrike) on Natanz at a time when the US feared further destabilizing the Middle East.[29] However, Israel likely needed little convincing. Just months before the discovery of the malware, the Israeli chief of military

[23] Shlomo Brom, "Is the Begin Doctrine Still a Viable Option for Israel?" in *Getting Ready for a Nuclear-Ready Iran*, eds. Henry Sokolski and Patrick Clawson (Carlisle [PA]: Strategic Studies Institute, US Army War College, 2005), pp. 133-158.
[24] John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy* 12, no. 2 (1993): p. 145.
[25] Rid, "Cyber War Will Not Take Place," pp. 17-18.
[26] Michael Joseph Gross, "A Declaration of Cyber-War", *Vanity Fair*, April 2011, quoted in Ibid., p. 6.
[27] Dan Williams, "Wary of Naked Force, Israelis Eye Cyberwar on Iran," *Reuters*, 7 July 2009.
[28] Barney Ward and Emily Fekete, "Relational Geographies of Cyberterrorism and Cyberwar," *Space and Polity* 20, no. 2 (2016): p. 149.
[29] David Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, 1 June 2012.

intelligence Major General Amos Yadlin said: "Using computer networks for espionage is as important to warfare today as the advent of air support was to warfare in the twentieth century." "The cyber-warfare field fits well with Israel's defense doctrine," he added.[30] The former assertion was repeated almost verbatim in *Maarachot*, the official journal of the IDF, in 2013. Colonel Nati Cohen opined: "In the early twenty-first century, where the whole world depends on the internet, supremacy in cyberspace may be as crucial as command of the air has been for most of the twentieth century […] Today cyberspace is where the air force was at the end of the First World War."[31] The two officers may have arrived at the analogy independently, though it is possible also that this was a meme within the IDF. Given the especial importance of airpower in Israeli military history—IDF staff colleges were likely inclined to repeat the tales of its decisive air superiority in the Six-Day War (1967)—the analogy speaks to a high value placed on cyber offence.[32] Top Israeli strategists evidently viewed cyber warfare not only as a new way of doing old tricks, but as a distinct domain that could define the century.

Charting a Path to Cyber Power

In the wake of the revelation of Stuxnet, the first comprehensive Israeli cyber-strategy was developed. Prime Minister Netanyahu claims that he was moved to action after reading a book that detailed a hypothetical cyberwar between China and the United States.[33] In 2010, Netanyahu asked a close confidant of his, retired Brigadier-General Isaac Ben-Israel, to head a formal review of Israeli cybersecurity.[34] Thus was born a taskforce called the National Cyber Initiative (NCI), which sought to answer, among other things, the question of how to ensure a place among the global top five

[30] "Israel Adds Cyber-Attack to IDF," *Defense Technology International*, 11 February 2010.
[31] Nati Cohen, "נרחבת סייבר למתקפת ישראל היערכות החמישי הממד" [The Fifth Dimension Is Israel's Preparedness for an Extensive Cyber Attack], *Maarachot*, 21 December 2013, pp. 10-11.
[32] Kenneth Pollack, "Air Power in the Six-Day War," *Journal of Strategic Studies* 28, no. 3 (2005): pp. 471-503.
[33] IsraeliPM, "PM Netanyahu Addresses CyberWeek 2018 Cybersecurity Conference," YouTube video, 16:18, https://www.youtube.com/watch?v=0HXEbGamgcQ; Considering the chronology, the book was likely Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2010).
[34] Tabansky and Ben-Israel, *Cybersecurity in Israel*, p. 43.

cyber powers by 2015.[35] After six months of consultations with some eighty experts, the NCI handed its report to the Prime Minister. The report is classified, though it has been described broadly as aiming "to provide [Israel] with superpower capabilities in cyberspace,"[36] to promote academic research on *cyber technology*, encourage everyday cyber security practices to the public, and above all to establish a national agency for cyber policy.[37] Another notable recommendation was for the creation of "a statewide protective shield."[38]

Following the report of the NCI, in 2011 the government adopted Resolution No. 3611, *Resolution on Advancing National Cyberspace Capabilities*, enshrining the National Cyber-Strategy of Israel stemming from the National Cyber Initiative.[39] The pursuit of the NCI's recommendations was difficult from the outset for political reasons, with different agencies and departments demanding greater say in cyber-strategy. Offices such as the Israel National Cyber Bureau (2012-2017) and the National Cyber Security Authority (2015-2018) came and went;[40] today all civilian cybersecurity is the responsibility of the Israel National Cyber Directorate (INCD).[41] The details always sort themselves out along the way, according to Prime Minister Netanyahu, with yet another army metaphor (perhaps we should expect these everywhere in a country with mandatory military service):

> We've decided to organize our national cyber effort in—what we say in the army is to move it in a direction and get everything organized as we move forward. In the military if you have a force in the field, you have a lot of tanks, armoured personnel carriers, or jeeps, they're scattered in the field, and you say 'well how am I going to push this thing forward?' And if you think about it and think about it and think about it, and think about every

[35] Lior Tabansky, "Cyberdefense Policy of Israel: Evolving Threats and Responses," *Chaire Cyber-Défense et Cyber-sécurité* (Paris, 2013), p. 4.
[36] Tabansky and Ben-Israel, *Cybersecurity in Israel*, p. 44.
[37] Tabansky, "Cyberdefense Policy of Israel," 4-5; Dmitry Adamsky, "The Israeli Odyssey toward its National Cyber Security Strategy," *The Washington Quarterly* 40, no. 2 (2017): p. 115.
[38] Tabansky, "Cyberdefense Policy of Israel," 5.
[39] United Nations Institute for Disarmament Research, "Cyber Policy Portal: Israel: Cybersecurity Policy," https://unidir.org/cpp/en/states/israel.
[40] Barak Ravid, "Battle Move in Israel's Cyber Turf War: Shin Bet Loses Authority Over 'Civilian Space'," *Haaretz*, 21 September 2014; Tabansky and Ben-Israel, *Cybersecurity in Israel*, p. 57.
[41] Israel National Cyber Directorate, website, https://www.gov.il/en/departments/israel_national_cyber_directorate.

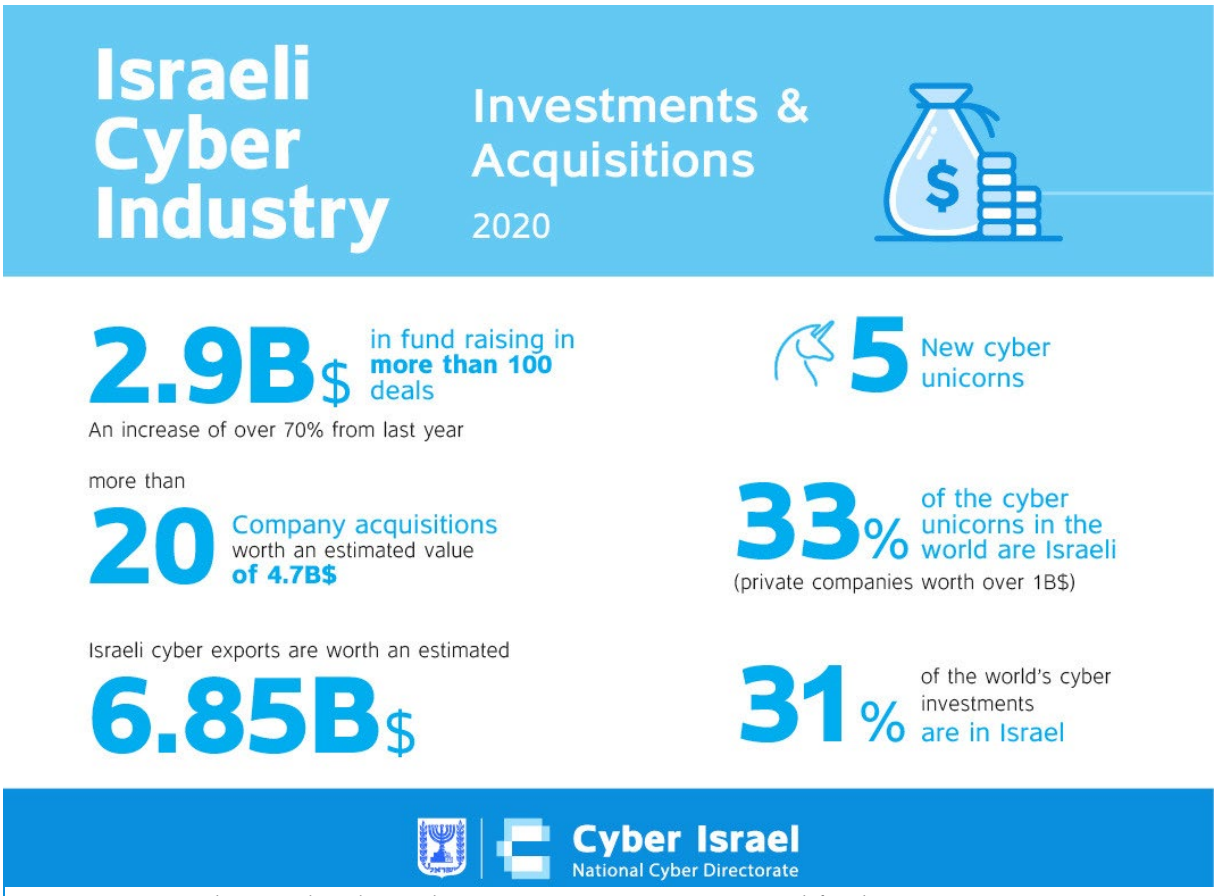
> individual piece and how they interconnect, you're not going to move. So what we do often in the military is we say we are moving in *that* direction, and everybody fall in place as we move forward. And in a way it's easier to organize things as you move forward.[42]

In other words: grand vision first, logistics later.

Global cyber power was, or is, *that* direction sought by Netanyahu. We need not be too strict about quantifying such a thing, and Netanyahu frequently repeats that it is a fast-moving target. A critical view would see his articulation of cyber power as a colloquial use of the term. The Israelis have incentivized investment and development in the IT private sector with great success, promoted cyber-literacy in education from a young age,[43] developed a robust national cyber security capacity, and evidently behind the scenes have a remarkable prowess in cyber offensive operations. The figures boasted by the INCD and touted by Netanyahu make clear that on one hand, being *a cyber power* is a national image rooted partly in metrics of less interest to scholars of military strategy:

[42] IsraeliPM, "PM Netanyahu's Full Remarks at CyberTech 2016," YouTube video, 27:20, www.youtube.com/watch?v=KqKfanu1e5w.
[43] Daniel Estrin, "In Israel, teaching kids cyber skills is a national mission," *Times of Israel*, 4 February 2017.

Figure 1: INCD on the Israeli Cyber Industry, 2020



Source: INCD, "The Israeli cyber industry continues to grow: record fundraising in 2020," 21 January 2021, https://www.gov.il/en/departments/news/2020ind.

Dima Adamsky draws a helpful conceptual distinction between Israel's *soft* cyber power and its *hard* cyber power. Netanyahu has tended to emphasize the soft power aspect—the economic and diplomatic benefits derived from Israeli prominence in the global private cyber industry.[44] But Israel has clearly invested substantial energy into developing *hard* cyber power as well. A conventional definition of cyber power in the strategic studies literature is provided by John Sheldon: "the ability in peace, crisis, and war to exert prompt and sustained influence in and from cyberspace."[45] The Israeli

[44] Adamsky, "The Israeli Odyssey toward its National Cyber Security Strategy," p.124.
[45] John Sheldon, "The Rise of Cyberpower," in *Strategy in the Contemporary* World, eds. John Baylis, James Wirtz, and Colin Gray (Oxford: Oxford University Press, 2016), p. 285.

conception of *hard* cyber power is congruent with this definition. The IDF's first official public doctrine from 2015 reads: "It is necessary to have simultaneous defense capability in all the operational arenas, in all Routine, Emergency and War situations and in all dimensions (ground, air, sea, and cyber)."[46] Notably, cyber warfare follows the concept of *Routine, Emergency, and War* (REW) in IDF doctrine applied across all other domains.

However, despite the wording, *defence capability* also implies an offensive power along the lines defined by Sheldon. The *R* in REW can also be a bellicose period according to the strategy of the Campaign Between Wars (CBW) formalized by the IDF in the aftermath of the 2006 Lebanon War. Following what was regarded as a poor performance in the war, the strategy of the CBW was intended to better prepare for future conflicts. Its aim is to delay wars by constantly weakening enemies and damaging their international legitimacy "in part by exposing clandestine military activities that violate international law."[47] Due to its inherently stealthy quality and because it has yet to meet the threshold for triggering a conventional war, a cyber attack is regarded as a key tool of the CBW. One article in *Maarachot* explained in 2013: "The unique features of cyberspace make it attractive for combat even in periods between conventional wars. Cyberattacks may be used […] [as] a means of exerting pressure to change the policy of the adversary in the periods between conventional wars [and] preventing emerging security threats."[48] Israeli military strategy blurs the line between war and peace to an extent greater than most states. Thomas Rid writes that "there is no known act of cyberwar, when war is properly defined."[49] Improperly defined though—that is, by the IDF rather than Carl von Clausewitz—Israel is always at war in some sense and has plenty of use for cyber weapons.

---

[46] Israel Defence Force, *Deterring Terror: How Israel Confronts the Next Generation of Threats: English Translation of the Official Strategy of the Israeli Defense Forces*, trans. Susan Rosenberg (Cambridge [MA]: Belfer Center for Science and International Affairs, 2016), p. 39.

[47] Gadi Eisenkot and Gabi Siboni, "The Campaign Between Wars: How Israel Rethought Its Strategy to Counter Iran's Malign Regional Influence," *Policy Watch* 3174 (Washington Institute for Near East Policy, 4 September 2019), https://www.washingtoninstitute.org/policy-analysis/campaign-between-wars-how-israel-rethought-its-strategy-counter-irans-malign.

[48] Cohen, "The Fifth Dimension Is Israel's Preparedness for an Extensive Cyber Attack," p. 11.

[49] Rid, "Cyber War Will Not Take Place," p. 15.

Exercising Cyber Power

Nations can endlessly devise doctrines and strategies for cyber space based on conventional military ideas. However, is this ever anything more than fanciful imagining or simply convenient metaphors for public consumption? Does cyber warfare *praxis* in Israel demonstrate anything distinctive based in national military doctrines or grand strategy?

All developed nations have some military and/or civilian capacity for cyber defence. Is there anything different about Israel's strategy for developing a statewide protective shield? It bears reminding that Israel's Iron Dome missile defence system was first deployed in March 2011, around the same time that the NCI submitted its report that would serve as the basis for a formal Israeli cyber strategy. Netanyahu began describing cyber defence in distinctly Israeli terms around 2012 when he told his Cabinet: "Just as we have the Iron Dome against missiles and the security fence against infiltrators and terrorism, we will have a similar protection against cyber-attacks."[50] Strategic analyst Michael Raska observed that

> one of the influential schools of thought in the Israeli cyber debate is discussing the applicability of the operational concepts and lessons learned from the Iron Dome missile defence methodology in the cyber domain. For example, how to create effective cyber intelligence (enemy analysis & target creation), early warning and absorption readiness, strike effort, area suppression, active defence, command and control, passive detection, and ultimately, cyber deterrence.[51]

Many Israelis besides Netanyahu are evidently enamoured with the idea of the *Cyber Iron Dome*, as this analogy has been made many times since 2012.[52] Indeed, as the

[50] Asher Zeiger, "Israel developing 'digital Iron Dome' to guard against cyberterrorism," *Times of Israel*, 14 October 2012.
[51] Michael Raska, "Building a Cyber Iron Dome: Israel's Cyber Defensive Envelope," *RSIS Commentary*, no. 192 (Oct. 2014): n.p.
[52] See Tel Aviv University, "Digital Warfare: TAU on the Frontline," 4 July 2013, https://english.tau.ac.il/events/cyber_conference; Benjamin Netanyahu, "PM Netanyahu addresses the 4th International Cybersecurity Conference," (Speech, Tel Aviv, 14 September 2014), https://mfa.gov.il/MFA/PressRoom/2014/Pages/PM-Netanyahu-addresses-the-4th-International-Cybersecurity-Conference-14 September 2014.aspx; Dan Arkin, "'Fully Prepared to Face the Threats'," *Israel Defense*, 27 May 2018.

head of the Israeli Electric Corporation said, comparing the cybersecurity situation to the "number of missiles fired by Hamas," Israeli energy infrastructure was hit by 15 "cyber-missiles a day" in 2014.[53]

The INCD claims that the Cyber Iron Dome is not yet complete, but concrete steps have been taken that arguably do resemble its kinetic counterpart.[54] For example, *Cybernet* is a new made-in-Israel social network that is conceived of as a decentralized nationwide array to stop or prevent cyber attacks. Users, typically cybersecurity professionals, share information on potential or ongoing cyberattacks for the benefit of other users and the government. Forums on the site are designed for exchanging information and advice, and safely uploading malicious files for analysis.[55] It is the first initiative of its kind and undoubtedly a creative approach to increasing resilience against cyberattacks on a national level, and it is tempting to see a conceptual influence from the array of radars and air defence missiles that constitute the Iron Dome. The Director of the INCD provides compelling evidence for this hypothesis, stating in 2017 (just as work on Cybernet was commencing): "If we look at the 'Iron Dome,' it does not protect a specific bank or energy company or some organization, but an entire nation. However, when you look at the cyber issue, most of the technologies and solutions aim towards defending a specific organization."[56] Cybernet addressed this problem by providing a network for organizations to cooperate with each other and with the government, hopefully shielding themselves from more 'cyber missiles' on a national scale rather than in an atomized way.

Israel's cyber-offensive capabilities naturally factor into the broad vision of cyber power. Cyber attack was readily justified by preexisting doctrines in Israeli military thought such as the interrelated concepts of deterrence, offensive defence, and the

---

[53] David Shamah, "A million hacks a day, but Israel's electric grid survives," *Times of Israel*, 24 March 2015.

[54] Grace Dennis, "Cybernet: A New Israeli Cybersecurity Social Network," *VPN Overview*, 20 January 2020.

[55] National Cyber Array, "סייבר תקיפות על מידע לשיתוף בעולם הראשונה החברתית הרשת - סייברנט" [Cybernet: The world's first social network for sharing information about cyber attacks], https://www.gov.il/he/departments/news/cybernet.

[56] Eviatar Matania, "Protecting a Country: Why Israel Created the National Cyber Directorate," *The Annual Cyber Security International Conference* (2017), https://icrc.m.tau.ac.il/sites/cyberstudies-english.tau.ac.il/files/media_server/cyber%20center/cyber-center/proceeding%202017.pdf.

CBW. This is a difficult subject to broach as the *known* instances of Israeli offensive cyber operations are presumably only the tip of the iceberg. They have, for example, used a cyber attack to disable Syrian air defence prior to a conventional attack, to sabotage Iranian nuclear enrichment facilities, and allegedly to hijack Lebanese telecommunications networks to spread anti-Hezbollah propaganda.[57] Offensive or active defence in Israeli strategic thought is particularly well suited for cyber attack. The Director of *Shin Bet*, Israel's domestic security intelligence agency, evidences this in a remark as revealing as it is cryptic: "In the real world we don't settle for passive defense, but rather strike the terrorists in their own territories, and the same goes for the cyber arena. We study the opponent's patterns of action, and know-how to strike them and surprise them, using a variety of ways and methods. Hackers all over the world, who act in order to harm Israel, experience unexpected malfunctions from time to time."[58]

We might tentatively suggest that there is a marked propensity to use cyber attack rooted in some idiosyncrasies of the Israeli geopolitical and military experience. Israel is one of the few countries in the world to acknowledge in a public strategic document that it has "destructive cyber capabilities."[59] But even without a Jabotinsky, Ben-Gurion, or Begin to draw from, the United States, the United Kingdom, Russia, and others conduct offensive operations in cyberspace against their strategic rivals in peacetime just as Israel does. Israel is not unique in this regard, but there are precedents in its conventional military strategy that explain why it sought to develop a reputation and offensive capacity in cyber space grossly disproportionate to its size and population.[60]

---

[57] Center for Strategic and International Studies, "Significant Cyber Incidents Since 2006," https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[58] Nadav Argaman, "Defending Israel's Cyber Borders," *The Annual Cyber Security International Conference* (2017), https://icrc.m.tau.ac.il/sites/cyberstudies-english.tau.ac.il/files/media_server/cyber%20center/cyber-center/proceeding%202017.pdf.

[59] Julia Voo et al., *National Cyber Power Index 2020: Methodology and Analytical Considerations* (Cambridge [MA]: Belfer Center for Science and International Affairs, 2020), p. 34.

[60] As the Director-General of the INCD said: "We are very small [but] cyberspace is where we can go to be much stronger and greater than our ratio in physical domain and population." See Journal of Middle Eastern Politics and Policy, "Event Review: Cyberspace: 'Everyone can attack everyone else'," blog post, 9 September 2016, https://jmepp.hkspublications.org/2016/09/09/cyberspace-everyone-can-attack-everyone-else/.

Conclusion

If cyber warfare is roughly where aerial warfare was in 1918, we have caught only a glimpse of its potential and are largely limited to theorizing until the next great confrontation. Netanyahu stayed true to the Israeli tendency going back to Ben-Gurion to prioritize advanced technologies in pursuit of a qualitative strategic advantage. Cyber space was incorporated into the official IDF strategy as a domain as discrete as land, air, or sea. Civilian agencies have ascribed equal importance to it as well. Whether waging conventional war or waging the *war between wars*, cyber offence is seen as an indispensable tool that furthers the traditional aims of Israeli strategy. Contending with cyber terrorism,[61] and cyber missiles, Israel defends its cyber borders[62] with a Cyber Iron Dome and wages cyber war in a manner that evidences a substantial conceptual importation from other domains. Nonetheless, like all other states it uses cyberwarfare in a complementary way. Therefore, cyber power only acquires real significance in a military sense when paired with power in the traditional domains.

What do we ultimately make of Israeli cyber power, *soft* metrics aside? A Weberian conception might have us examining the extent to which Israel is able to use and target "computers, networks, or other technologies" [63] against enemy countermeasures whilst its own countermeasures prohibit enemies from doing the same. A key difference in cyber space, however, is that offensive capabilities are not necessarily useful for defence.[64] One cannot meaningfully impose their will in cyber space if they are as likely to be hacked as they are to hack. One might amass armed men, boats, and planes and expect to accrue power in land, sea, and air respectively—but a legion of skilled hackers or cyber-saboteurs is not analogous in cyber space. More qualified people have tried and failed to measure Israel's capabilities separately in cyber defence and cyber offence. The *National Cyber Power Index 2020* from the Harvard Kennedy School rates the ostensible components of cyber power: surveillance, cyber defence, information control, intelligence gathering, technological competence,

[61] For one dramatic example see Toi Staff, "Next 9/11 will be caused by hackers, not suicide bombers, cyber expert warns," *Times of Israel*, 15 April 2015.
[62] Argaman, "Defending Israel's Cyber Borders," *The Annual Cyber Security International Conference* (2017).
[63] Cohen, Friedlich, and Siboni, "Israel and Cyberspace: Unique Threat and Response," p. 309.
[64] This is a point made by Thomas Rid. See NATO, "Cyberwar – does it exist? (NATO Review)," YouTube video, 2:52, https://www.nato.int/docu/review/articles/2013/06/13/cyberwar-does-it-exist/index.html.

destroying/disabling enemy infrastructure, and defining international norms. Israel, it admits, ranks too low by their metrics (11th overall in national comprehensive cyber power), likely in part because the open-source data that informed the report could not do justice to the highly covert nature of Israel's cyber program.[65] Israel: a top five global cyber power? Frankly, we do not know. They probably prefer to keep it that way.

[65] Voo et al., *National Cyber Power Index 2020: Methodology and Analytical Considerations*, pp. 41-42.

BIBILIOGRAPHY

"Israel Adds Cyber-Attack to IDF," *Defense Technology International*, 11 February 2010.

Adamsky, Dmitry. "The Israeli Odyssey toward its National Cyber Security Strategy." *The Washington Quarterly* 40, no. 2 (2017): pp. 113-127.

Alberto Gomez, Miguel. "Overcoming uncertainty in cyberspace: strategic culture and cognitive schemas." *Defence Studies* 21, 1 (2021): pp. 25-46.

Argaman, Nadav. "Defending Israel's Cyber Borders." *The Annual Cyber Security International Conference* (2017), https://icrc.m.tau.ac.il/sites/cyberstudies-english.tau.ac.il/files/media_server/cyber%20center/cyber-center/proceeding%202017.pdf.

Arkin, Dan. "'Fully Prepared to Face the Threats'." *Israel Defense*, 27 May 2018.

Arquilla, John, and David Ronfeldt. "Cyberwar is Coming!" *Comparative Strategy* 12, no. 2 (1993): pp. 141-165.

Bar, Shmuel. "Israeli Strategic Deterrence Doctrine and Practice." *Comparative Strategy* 39, no. 4 (2020): pp. 321-353.

The Blavatnik Interdisciplinary Cyber Research Center, TAU. "Main Plenary – Prime Minister of Israel, Mr. Benjamin Netanyahu." YouTube video, 8:44, https://www.youtube.com/watch?v=QVh7uEWP4ik.

Branch, Jordan. "What's in a Name? Metaphors and Cybersecurity," *International Organization* 75 (2021): pp. 39-70.

Brom, Shlomo. "Is the Begin Doctrine Still a Viable Option for Israel?" In *Getting Ready for a Nuclear-Ready Iran*, pp. 133-158. Edited by Henry Sokolski and Patrick Clawson. Carlisle [PA]: Strategic Studies Institute, US Army War College, 2005.

Center for Strategic and International Studies. "Significant Cyber Incidents Since 2006." https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Cohen, Matthew, Charles Freilich, and Gabi Siboni. "Israel and cyberspace: Unique threat and response." *International Studies Perspectives* 17, no. 3 (2016): pp. 307-321.

Cohen, Nati. "נרחבת סייבר למתקפת ישראל היערכות החמישי הממד" [The Fifth Dimension Is Israel's Preparedness for an Extensive Cyber Attack]. *Maarachot*, 21 December 2013.

Colomb, Philip Howard. *Naval Warfare, Its Ruling Principles and Practice Historically Treated.* London: W.H. Allen and Co. Ltd., 1891.

Cristiano, Fabio. "Israel: Cyber Defense and Security as National Trademarks of International Legitimacy." In *Routledge Companion to Global Cyber-Security Strategy*, edited by Scott Romaniuk and Mary Manjikian, pp. 409-417. New York: Routledge, 2020.

Dennis, Grace. "Cybernet: A New Israeli Cybersecurity Social Network." *VPN Overview,* 20 January 2020.

Douhet, Giulio. *Command of the Air*. Translated by Dino Ferrari. Alabama: Air University Press, 2019.

Eisenkot, Gadi, and Gabi Siboni. "The Campaign Between Wars: How Israel Rethought Its Strategy to Counter Iran's Malign Regional Influence." *Policy Watch* 3174. Washington Institute for Near East Policy, 4 September 2019, https://www.washingtoninstitute.org/policy-analysis/campaign-between-wars-how-israel-rethought-its-strategy-counter-irans-malign.

Estrin, Daniel. "In Israel, teaching kids cyber skills is a national mission." *Times of Israel*, 4 February 2017.

Handel, Michael. "The evolution of Israeli strategy: The psychology of insecurity and the quest for absolute security." In *The Making of Strategy: Rulers, States, and War*, edited by Williamson Murray, Alvin Bernstein, and MacGregor Knox, pp. 534-578. Cambridge: Cambridge University Press, 1999.

Israel Defence Force. *Deterring Terror: How Israel Confronts the Next Generation of Threats: English Translation of the Official Strategy of the Israeli Defense Forces*. Translated by Susan Rosenberg. Cambridge [MA]: Belfer Center for Science and International Affairs, 2016.

Israel, Prime Minister's Office, Resolution no. 3611 "Promoting National Capacity in Cyberspace," 7 August 2011, https://www.gov.il/he/departments/policies/2011_des3611.

Israel National Cyber Directorate. "The Israeli cyber industry continues to grow: record fundraising in 2020." 21 January 2021, https://www.gov.il/en/departments/news/2020ind.

IsraeliPM. "PM Netanyahu's Full Remarks at CyberTech 2016." YouTube video, 27:20, www.youtube.com/watch?v=KqKfanu1e5w.

IsraeliPM. "PM Netanyahu Addresses CyberWeek 2018 Cybersecurity Conference." YouTube video, 16:18, https://www.youtube.com/watch?v=0HXEbGamgcQ.

Jokisipilä, Markku. "E-Jihad, Cyberterrorism and Freedom of Speech." In *War, Virtual War and Society: The Challenge to Communities*, pp. 89-113. Edited by Andrew Wilson and Mark Perry. Amsterdam: Brill, 2008.

Journal of Middle Eastern Politics and Policy. "Event Review: Cyberspace: 'Everyone can attack everyone else'." Blog post. 9 September 2016, https://jmepp.hkspublications.org/2016/09/09/cyberspace-everyone-can-attack-everyone-else/.

Matania, Eviatar. "Protecting a Country: Why Israel Created the National Cyber Directorate." *The Annual Cyber Security International Conference* (2017), https://icrc.m.tau.ac.il/sites/cyberstudies-english.tau.ac.il/files/media_server/cyber%20center/cyber-center/proceeding%202017.pdf.

National Cyber Array. "סייבר תקיפות על מידע לשיתוף בעולם הראשונה החברתית הרשת - סייברנט" [Cybernet: The world's first social network for sharing information about cyber attacks], https://www.gov.il/he/departments/news/cybernet.

NATO. "Cyberwar – does it exist? (NATO Review)." YouTube video, 2:52, https://www.nato.int/docu/review/articles/2013/06/13/cyberwar-does-it-exist/index.html.

Netanyahu, Benjamin. "PM Netanyahu addresses the 4th International Cybersecurity Conference." Speech, Tel Aviv, 14 September 2014, https://mfa.gov.il/MFA/PressRoom/2014/Pages/PM-Netanyahu-addresses-the-4th-International-Cybersecurity-Conference-14-Sep-2014.aspx.

Netanyahu, Benjamin. "Prime Minister Benjamin Netanyahu's Remarks at the Cyber-Tech Conference." Speech, Tel Aviv, 31 January 2017, https://www.gov.il/en/departments/news/speechtech310117.

Oren, Aniram, Oren Barak, and Assaf Shapira. "'How the Mouse Got His Roar': The Shift to an 'Offensive-Defensive' Military Strategy in Israel in 1953 and Its Implications." *The International History Review* 35, no. 2 (2013): pp. 356-376.

Pollack, Kenneth. "Air Power in the Six-Day War." *Journal of Strategic Studies* 28, no. 3 (2005): pp. 471-503.

Raska, Michael. "Building a Cyber Iron Dome: Israel's Cyber Defensive Envelope." *RSIS Commentary*, no. 192 (October 2014): n.p.

Ravid, Barak. "Battle Move in Israel's Cyber Turf War: Shin Bet Loses Authority Over 'Civilian Space'." *Haaretz*, 21 September 2014.

Rid, Thomas. "Cyber War Will Not Take Place," *Journal of Strategic* Studies 35, no. 1 (2012): pp. 5-32.

Sanger, David. "Obama Order Sped Up Wave of Cyberattacks Against Iran." *New York Times*, 1 June 2012.

Shamah, David. "A million hacks a day, but Israel's electric grid survives." *Times of Israel*, 24 March 2015.

Sheldon, John. "The Rise of Cyberpower." In *Strategy in the Contemporary World*, edited by John Baylis, James Wirtz, and Colin Gray, pp. 282-298. Oxford: Oxford University Press, 2016.

Staff, Toi. "Next 9/11 will be caused by hackers, not suicide bombers, cyber expert warns." *Times of Israel*, 15 April 2015.

State Comptroller of Israel, "Using Information Technology to Provide Government Services to the Public." April 2003, https://www.mevaker.gov.il/he/Reports/Report_361/1e0d9521-0679-4b03-ad7d-11d546604a29/InformationTechnology_and_eGovernment53b.pdf.

Tabansky, Lior. "Cyberdefense Policy of Israel: Evolving Threats and Responses." *Chaire Cyber-Défense et Cyber-sécurité.* Paris, 2013.

Tabansky, Lior, and Isaac Ben Israel. *Cybersecurity in Israel*. New York: Springer, 2015.

Tabansky, Lior. "Israel Defense Forces and National Cyber Defense." *Connections* 19, no. 1 (2020): pp. 45-62.

Tel Aviv University. "Digital Warfare: TAU on the Frontline." 4 July 2013, https://english.tau.ac.il/events/cyber_conference.

Trendle, Giles. "Cyberwars: The coming Arab E-Jihad." *The Middle East* (April 2002).

United Nations Institute for Disarmament Research. Cyber Policy Portal, Israel, Cybersecurity Policy. https://unidir.org/cpp/en/states/israel.

Voo, Julia, Irfan Hermani, Simon Jones, Winnona DeSombre, Daniel Cassidy, and Anina Schwarzenbach. *National Cyber Power Index 2020: Methodology and Analytical*

Considerations. Cambridge [MA]: Belfer Center for Science and International Affairs, 2020.

Ward, Barney, and Emily Fekete. "Relational Geographies of Cyberterrorism and Cyberwar." *Space and Polity* 20, no. 2 (2016): pp. 143-157.

Weber, Max. *Economy and Society: An Outline of Interpretive Sociology*. Edited by Guenther Roth and Claus Wittich. Berkeley: University of California Press, 1978.

Williams, Dan. "Wary of Naked Force, Israelis Eye Cyberwar on Iran." *Reuters*, 7 July 2009.

Zeiger, Asher. "Israel developing 'digital Iron Dome' to guard against cyberterrorism." *Times of Israel*, 14 October 2012.