CYBERDEFENSE REPORT

Israel's National Cybersecurity and Cyberdefense Posture

Policy and Organizations

Zürich, September 2020

Cyber Defense Project (CDP)
Center for Security Studies (CSS), ETH Zürich

CSS ETH Zurich

ETH zürich

Available online at: css.ethz.ch/en/publications/risk-and-resilience-reports.html

Author: Jasper Frei

ETH-CSS project management: Myriam Dunn Cavelty, Deputy for Research and Teaching; Benjamin Scharte, Head of the Risk and Resilience Team; Andreas Wenger, Director of the CSS.

Layout and graphics: Miriam Dahinden-Ganzoni
Editor: Sean Cordey

DOI: 10.3929/ethz-b-000438397

Abstract

This report provides a brief overview of Israel's national cybersecurity and cyberdefense posture. It outlines key focusing events that have influenced Israel’s threat perception and lays out the evolution and various shifts of its cybersecurity and defense policy. It also provides an overview of the national organizational framework, summarizes key strategy documents as well as describes its main international and national partnerships.

Table of Contents

Highlight/Summary

1. Key National Trends

Israel, with its innovative and well-funded tech scene and pro-active military/ intelligence apparatus, is one of the most advanced cybersecurity and cyberdefense players in the world. Its geopolitical position has led it to develop and use its sophisticated intelligence and offensive capabilities to support its conventional military operations and project power in the region. This strive for security has also led it to reinforce its strategic partnership with the US and somewhat engage in the international norms building processes for cyberspace.

2. Key Policy Principles

2.1 Cybersecurity

Israel has adopted a comprehensive cybersecurity policy approach with a specific focus on developing cyber robustness, cyber resilience, and capacity. This is done in close coordination with national and international public and private stakeholders. Cybersecurity is seen as having key potential for Israel's economy and innovation.

2.2 Cyberdefense

Active cyberdefense and defensive operations are two core pillars of Israel's 2017 cybersecurity strategy. The IDF's approach is also driven by four of Ben Gurion's doctrinal principles: deterrence, decisive victory, early warning, and alliances. Its capabilities are developed in response to explicitly mentioned enemies, such as Syria, Iran, Lebanon, Hezbollah, Hamas, and ISIS.

3. Key National Frameworks

3.1 Cybersecurity

Israel's strategic cybersecurity policy is led and coordinated at the top by the Israeli National Cyber Directorate (INCD), which is directly under the direct aegis of the Prime Minister and his office. The INCD combines the tasks of the former National Cyber Security Authority (NCSA), which had an operational orientation, and the more policy-oriented Israel National Cyber Bureau (INCB). At the operational level, efforts are divided according to issue areas between Mossad, Shin bet, the Israel Police, and the INCD. In practice, these agencies have exhibited differing core values and operational approaches that have created friction with the INCD.

3.2 Cyberdefense

The Israeli Defense Forces (IDF) main cyberdefense organs are its Unit 8200 (for offensive cyber operations) and the C4I Directorate (for defensive operations and infrastructure security). Shin Bet, Mossad, the Israel Police, and the Ministry of Justice are also involved. They collaborate with and are coordinated by the INCD.

4. Level of Partnerships and Resources

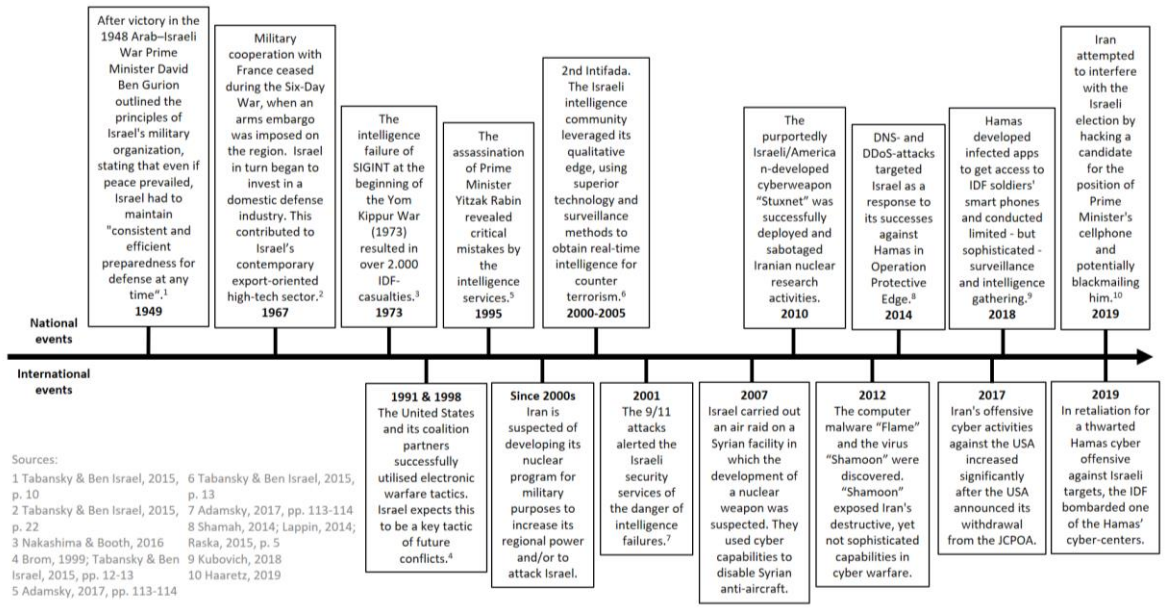
Israel's government has actively engaged the academia and the private sector to improve its R&D. Its largest partnership is an innovation park: Cyberspark. Internationally, its closest partner remains the US and its NSA.

1 Evolution of Israel's National Cybersecurity Policy

1.1 Threat Perceptions: Trigger Events

Diagram 1 provides an overview of the domestic and international events that influenced Israel's threat perception and shaped its cybersecurity and cyberdefense policies.

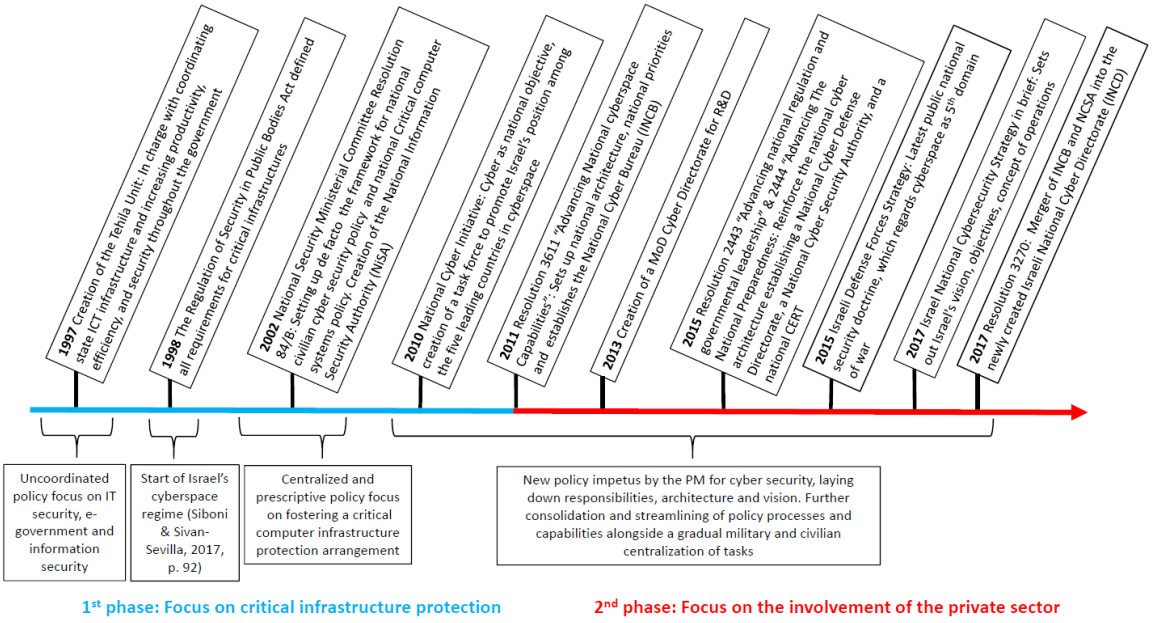
Diagram 1. Timeline of Trigger Events



1.2 Main Policy Documents: Evolution and Key Shifts

Diagram 2 provides an overview of the evolution of Israel's cybersecurity and cyberdefense policies since the 90s.

Diagram 2. Timeline of Policy Developments and Shifts



1.3 Organizational Structures: Key Parameters

Critical infrastructure protection (CIP) was the primary motivation behind the early Israeli civilian cybersecurity efforts. Instead of coordinated efforts, solutions were at first reached on a short-term, pragmatic, and ad-hoc basis. These choices resulted in a relatively decentralized system. However, in the last couple of years, the Israeli government has put significant effort into unifying the different civilian cybersecurity agencies into one single entity, called the Israel National Cyber Directorate (INCD).

The INCD's is part of the Israeli Prime Minister's Office. Only three other agencies – i.e. Shin Bet, Mossad, and the Israeli Atomic Energy Committee – are directly subordinated to the Prime Minister's Office (PMO). This tends to show how essential the INCD is perceived to be to Israel's security (Adamsky, 2017, p. 120). Its mandate is to organize the civilian cybersecurity landscape. It thus coordinates all aspects of civilian cyberdefense, ranging from operational defense to building technological capacities and policy proposals. The INCD combines the tasks of the former National Cyber Security Authority (NCSA), which had an operational orientation, and the more policy-oriented Israel National Cyber Bureau (INCB) (gov.il, 2018). Some civilian cybersecurity tasks remain outside of the INCD's scope, such as those functions which require the input and capacities of the Israel Police or the intelligence services (ibid.).

There is a clear tendency towards the centralization of the formerly decentralized civilian cybersecurity landscape. Civilian cybersecurity is complemented by military cyberdefense, which is under the aegis of the Israel Defense Forces (IDF). The IDF's Unit 8200 is responsible for offensive tasks while the C4I Directorate focuses on defensive measures. However, organizational leadership can shift. In peacetime, the INCD is responsible for civilian national defense campaigns while the IDF takes the lead to implement offensive and defensive campaigns on the national level in emergencies or times of war (Adamsky, 2017, p. 120).

1.4 Context/Analysis: Key National Trends

Israel is a regional power with a thriving economy who has been facing critical threats to its national security since its formation. In the last decades, it has been showing a willingness to project power through military operations and interference in neighboring wars. Israel is also allegedly in possession of nuclear capacities. Today, Israel's main adversaries are: states (Iran and Lebanon), failing and failed states (Syria), state-like entities (Hamas and Hezbollah) as well as terrorist organizations without links to a specific country or community (ISIS and the Palestinian Islamic Jihad) (Eizenkot, 2016, p. 4). Domestic challenges, such as political tensions caused by ethnic, religious, and historical divides, also threatened Israel's stability. Besides, allegations of corruption in politics and socio-economic inequality have also caused some civil unrest.[1]

The focus on projecting power to defend its state has, to a certain extent, transitioned from traditional military domains to the cyber one. Today, Israel views itself as one of the five most powerful states in terms of cyber (Netanyahu, 2018). This perception rests on two pillars: (1) a strong and pro-active military and a robust intelligence services as well as (2) an innovative civilian sector.

Concerning the former, the IDF deploys its cyber capabilities in sophisticated cyberattacks (e.g. Stuxnet (see Baezner & Robin, 2017)) or espionage campaigns (e.g. Flame and Duqu (see Symantec, 2011; Katz, 2012)). The domestic intelligence community (Shin Bet and Mossad), meanwhile, integrates cyber in its approach to strengthen domestic security by engaging in significant information sharing processes with various governmental bodies. Intelligence and offensive cyber capabilities are also applied to support the conventional military sector. This proactive approach to protect the State of Israel and its sovereignty can be observed throughout Israel's military history and is outlined in its current IDF defense strategy (Eizenkot, 2016).

Additionally, as part of the countries' longstanding strategic partnership with the US, Israel maintains strong ties with US cyberdefense agencies. However, despite being considered a major strategic partner to NATO, having good relations with Russia, strengthening ties with India, and its past military cooperation with the United Kingdom and France during the Suez Crisis, Israel does not have any formal allies with binding commitments. As a result, Israel is under pressure to develop powerful military capabilities to deter its adversaries. Added to that, both the mandatory military service and the IDF's focus on technological superiority have been instrumental in shaping the development of Israel's cyber capabilities.

Concerning the latter, there are significant investments in civilian cyber capabilities. Even though Israel's economy faces various difficulties, globally, it still ranks 31st in terms of GDP per capita (OECD, 2019a). It spends six to eight per cent of its GDP for defense (Tabansky & Ben Israel, 2015, p. 17), but also tops the world in terms of gross domestic spending on research and development relative to GDP, spending more than 4.5 per cent of its GDP on it (OECD, 2019b). This emphasis on research and development, as well as the

[1] This is a selection of a multitude of political challenges Israel faces and does not claim to be exhaustive.

stimulating role of the IDF's technical units (e.g. Unit 8200), provide a fertile environment for a thriving start-up and high-tech-sector (Breznitz, 2002; Efrat, 2014; Swed & Butler, 2015). Cultural values (e.g. innovativeness, creativity, criticism across hierarchy levels), which were shaped by significant immigration, further facilitate innovation (Senor & Singer, 2011; Tabansky & Ben Israel, 2015, p. 18). Receiving approximately 20 per cent of global investment in cybersecurity (815 million USD), Israel's 420 cybersecurity companies earn 3.8 billion USD in exports (Netanyahu, 2018; Start-up Nation Central) or eight per cent of the global market of cybersecurity solutions (Tsipori, 2016; Housen-Couriel, 2017, p. 5).

In terms of international efforts, Israel was a member of the fifth United Nations' Group of Government Experts (UN GGE) in the field of information and telecommunications and the Geneva Dialogue on Responsible Behavior in Cyberspace, and thereby participated in setting norms for acceptable state behavior in cyberspace (United Nations General Assembly, 2018; Cornish & Kavanagh, 2019, p.25). Israel is also a signatory to the Council of Europe's Convention on Cybercrime (Council of Europe, 2019) and established bilateral cooperative relationships (e.g. with the US (congress.gov, 2016), Bulgaria (Times of Israel, 2018), and Australia (ADM, 2017)).

2 Current Cybersecurity Policy

2.1 Overview of Key Policy Documents

Perhaps surprisingly, a state with such a robust national defense policy does not have a formal national security strategy (Freilich, 2018, p. 1). In fact, Israel's leadership generally avoids publishing any declarative documents, whether by choice or constraints (Tabansky & Ben Israel, 2015, p. 4). Indeed, in the past, attempts to formulate a national security strategy did not succeed due to considerable political and bureaucratic obstacles. Instead of relying on formalized planning processes, Israeli security efforts thus tend to be pursued on a more ad-hoc basis (Freilich, 2018, p. 2). The most relevant strategies and policy documents are detailed below.

2.1.1 Israel's Doctrinal Principles by David Ben Gurion, 1953

Despite not being formalized in official publications, the overarching doctrinal principles of Israel's security policy are well known. The late Prime Minister David Ben Gurion presented them in his 18 October 1953 report to the Cabinet. The Israeli political and defense establishment dynamically adapted those principles ever since (Tabansky & Ben Israel, 2015, p. 4). This grand strategy – *Tfisat HaBitachon* – was conceived over 65 years ago in a different security context: a young nation, exhausted from the Israeli-Arab War, and under threat of an invasion by its Arab neighbors. Still, these doctrinal principles are the closest Israel has ever gotten to a formal national security strategy (Freilich, 2018, p. 2). These principles and Ben Gurion's 1948 call for Israel to maintain "consistent and efficient preparedness for defense at any time" even after the fighting ended, are still relevant for today's cybersecurity and cyberdefense strategies (Tabansky & Ben Israel, 2015, p. 10). Summarizing these principles, Ben Gurion ordered the Israeli military to put its efforts into (Ben Gurion, 1953; Tabansky & Ben Israel, 2015, p. 11):

1. The defense of the state, its residents, infrastructure, and interests.
2. The deterrence of potential attacks.
3. The formation of alliances with great powers.
4. The development of sophisticated early warning capabilities to compensate Israel's lack of strategic depth.
5. To achieve technological superiority and a qualitative edge to compensate for Israel's lack of critical resources.
6. To ensure rapid and decisive victory in case of a confrontation.

2.1.2 Eizenkot's IDF Strategy, 2015

In 2015, the IDF, under the leadership of former chief of General Staff Gadi Eizenkot, "published its first-ever public defense doctrine" that included, among others, its perspective on the use of cyber capabilities (Eizenkot, 2016). Specifically, this strategy acknowledges the enemies' development of cyber capabilities as well as the cyber domain as one of the four relevant domains to Israel's defense (next to land, sea, and air). The strategy also regards cyber capacities as integrated support for conventional defense and offense at all levels of combat (i.e. strategic, operative, and tactical). The IDF considers military cyberdefense and offense as vital to ensure: the functioning of the state and IDF institutions, the utilization of intelligence, collective defense, influence operations, and achieving legitimacy as well as legal responses. Finally, this strategy emphasizes strategic and tactical deterrence via cyberwarfare (Eizenkot, 2016).

2.1.3 Israel National Cyber Security Strategy, 2017

Before 2017, Israel had never formulated a comprehensive, official national cybersecurity strategy. This strategy by the INCD is the first Israeli national security white paper since Ben Gurion's 1953 declaration of strategic principles (Adamsky, 2017, p. 122). This short document describes the priorities of the INCD. Apart from general common goals – e.g. the goal to defend Israel's economic and social strength – it does not relate much to Eizenkot's 2015 IDF strategy. Specifically, it describes how Israel plans to improve its cyber robustness, systemic resilience, civilian national cyberdefense, and outlines the establishment and tasks of the NCSA. Finally, it also touches upon capacity building and international cooperation (INCD, 2017).

2.1.4 Preliminary Governmental Resolutions

Before the 2017 cybersecurity strategy, various governmental resolutions[2] have attempted to order Israel's cybersecurity landscape. The following table (Table 1) describes them in more detail.

[2] Governmental resolutions, in the Israeli context, are akin to binding executive orders. They are decided by a consensus of the whole Israeli government/ cabinet and generally needs to be backed by budgetary agreements between the involved ministries and the budget department.

Table 1. List of Governmental Resolutions Regulating Israel's Cybersecurity Landscape

Resolution	Description / Goals	Sources

84/B (2002)	• One of the first Critical Infrastructure Protection (CIP) policy concepts in the world, it tasked the National Information Security Authority (NISA or *Re'em*) and the policy-oriented steering committee with the implementation of CIP.
	• Rational behind mandating the Shin Bet with CIP:
	  ○ The Israeli government needed a quick and effective solution in the high-tension period of the Second Intifada (2000-2005).
	  ○ The expertise already existed within this organization.
	• Problem: NISA was part of Shin Bet and, as such, had not only vast authority but also considerable access to information and discretionary power over security matters. Besides, the cost of the imposed measures had to be covered by the supervised organizations. Overall, the intelligence agency seemed to stifle innovation and economic growth.
		Tabansky & Ben Israel, 2015, p. 38; Tabansky, 2011; Adamsky, 2017, p. 115

3611 (2011)	• Goals: Achieve technological, diplomatic, and economic progress as well as maintain status as a global cyber power.
	• Included various stakeholders and balanced governmental and private corporations' interests (this marked a stark contrast and improvement to Resolution 84/B).
	• Established the INCB and outlined how research and defensive cyber capabilities should be advanced. The INCB's mandate and objectives (i.e. 27 goals) can be synthesized as follows :
	  ○ Research, development, and operationalization of national security capabilities and technologies. This should result in centralized security services, information sharing platforms, and solutions for national efforts to expose, investigate, and contain cyberattacks.
	  ○ Promote innovation and research by industry and academia and enhance the nation's cyber-specific human capital.
		Tabansky & Ben Israel, 2015, p. 54; Adamsky, 2017, p. 115; Prime Minister's Office, 2011; INCD, 2017, p. 17

2443 (2015)	• Established the NCSA as an operative agency, which acts alongside the INCB. • Goal: To provide legal frameworks for the intelligence community's activities (i.e. balance basic freedom, privacy, and civil rights) and support businesses that lack human and financial resources. • Established CERT-IL and its various sectorial CERTs • NCSA took over CIP tasks from Shin Bet (except the communication bodies).	Tabansky & Ben Israel, 2015, pp. 58-59; Prime Minister's Office, 2015a; Prime Minister's Office, 2015b; gov.il, 2018; Shtokhamer, 2018; Ziv, 2018
2444 (2015)	• Tasked the NCSA with developing a national cyber doctrine • Outlined the development of international cooperation, public relations, licensing, auditing, training, instruction, and regulations.	
3270 (2017)	• Created the INCD, which unites NCSA and INCB	gov.il, 2017

2.2 National Cybersecurity Strategy: Fields, Tasks, and Priorities

The National Cybersecurity Strategy (INCD, 2017) is Israel's first comprehensive official cyber strategy. It includes both direct state actions to confront cyber risks as well as indirect efforts, which aim at supporting and collaborating with the private sector. This comprehensive strategy marks a shift from earlier policy decisions, which focused on solving pressing problems rather than outlining the bigger picture. The following paragraphs summarize the strategy's three parts.

2.2.1 Concept of Operations

The first part pertains to civilian cyberdefense activities and consists of three layers:

1. Fostering an **"aggregated cyber robustness"** against daily threats, thus preventively reducing risks. As outlined by the 2015 Government Resolution 2443, the state promotes – e.g. with incentives, regulations, best practice, or guidance – security efforts undertaken by the private sector. Regulations are mainly applied to the supply side of cyber products and services; the INCD sets mandatory standards for essential sectors and critical infrastructure. On the demand side, it sponsors awareness raising and knowledge promotion throughout the private sector.
2. Cultivating a **"systemic cyber resilience,"** mainly through improving inter-governmental and international cooperation as well as incident response. Systemic resilience is event-driven and reactive, regardless of specific events. The general efforts consist of intelligence gathering and sharing of sector-relevant information, sectoral centers, early warning mechanisms, incident response capabilities, and call centers. CERT-IL coordinates systemic cyber resilience efforts by collaborating with the private sector through sector-based cyber centers as well as by directly supporting companies at risk and cooperating on the local and global levels.
3. Enhancing civilian **"national cyberdefense"** to mitigate the most severe cyber threats to national security. It relies on the two preceding layers and includes not only defensive measures (e.g. defensive operations by CERT-IL and situation assessment) but also active cyberdefense and offensive actions by national security and law enforcement organs to counter both state and non-state aggression to achieve deterrence (INCD, 2017, pp. 9-13).

The first layer is a challenge that organizations need to solve themselves without substantive assistance from the state. Responsibilities shifts from the private sector to the government the higher the threat level becomes. The third layer is the exclusive task of state authorities.

2.2.2 Capacity Building

The second part outlines educational and industrial efforts for capacity building, which build the foundation for cyber operations. It describes plans to improve the national cyber ecosystem: stimulation of state-owned industries and commercial R&D, academic research, and education from first grade to university as well as supporting the development of prospective dual-use technologies that can be used by the state (INCD, 2017; Adamsky, 2017, pp. 115-118).

2.2.3 Structures

The third part details the configuration and mandate of the INCD, which oversees the implementation of the concepts outlined in the first two parts and unifies the responsible institutions for all three layers (i.e. robustness, resilience, and defense). The INCD is also responsible for international coordination and formulation of a legal framework for cyber issues. It also coordinates national cyberdefense efforts with military and security agencies. The IDF, meanwhile, integrates offensive and defensive campaigns in the event of an emergency (INCD, 2017; Adamsky, 2017, pp. 115-118).

***

There is no publicly available implementation plan for the 2017 National Cybersecurity Strategy. Various projects by the INCD, however, seem to flesh some of its aspects out. This includes projects such as "High Castle," "Crystal Ball," "Showcase," and "Cybernet+." These aim at improving Israel's capacity to detect and prevent cyber incidents, enhance coordination and intelligence, increase readiness and risk management, and facilitate data sharing and distribution processes across institutions.

"High Castle," for instance, is a platform for governmental and private stakeholders to improve detection, investigation, and blocking capabilities. "Crystal Ball," meanwhile, combines various threat intelligence collection tools, adds the findings from "High Castle" and creates a unified threat projection to improve situation analysis capabilities for intelligence services and civilian stakeholders. "Showcase" evaluates risk exposure and the degree of preparedness in critical infrastructure. It also recommends steps for improvement. Lastly, "CyberNet+" is a public-private

partnership information exchange platform that allows anonymous sharing of threats (Zack, 2018). These projects do not constitute a comprehensive strategy but are tailored to improve some of the most pressing cybersecurity problems Israel faces.

2.3 National Cyberdefense Strategy

Even though the IDF is considered one of the most "cyber capable" armies, Israel does not have a dedicated and public cyberdefense strategy. The (civilian) National Cybersecurity Strategy of 2017, however, lays out the defensive and offensive capabilities of the IDF. It also advocates for flexible leadership and oversight between the IDF and the INCD. Despite the lack of implementation plan, strategic objectives are known to be implemented by at least two organizations, namely C4I Directorate (for cyberdefense) and Unit 8200 (for cyberoffense). The 2015 IDF strategy does not elaborate on cyberdefense, but it states that cyber has a supportive function for IDF operations (Eizenkot, 2016, p. 22).

Additionally, the IDF applies at least four of Ben Gurion's doctrinal principles in its cyberdefense strategy:

1. **Deterrence** is rather challenging to achieve in cyberspace. To implement Ben Gurion's plan to deter Israel's enemies from attacking, Uri Tor (2017) introduced the concept of "cumulative deterrence." According to this approach, which is widely applied in IDF's conventional branches, deterrence needs to be "recharged" by sporadic outbreaks of violence to respond to aggression. The IDF has set a precedent when it reacted in real-time to a cyberattack by bombing Hamas' cyber headquarter, thus providing "a glimpse of the future of warfare" (IDF, May 5, 2019; Groll, 2019).
2. **Decisive victory** has achieved limited success. Even though Israel's Unit 8200 carried out various sophisticated cyberattacks, none have yet achieved a decisive victory on its own. They have instead supported intelligence collection (e.g. with "Flame") or sabotage (e.g. with "Stuxnet").
3. **Early warning** proved to be successful through cyberspace means. Indeed, Unit 8200 did provide several early warnings that helped prevent domestic terror attacks and predict foreign aggressions. Some doubts remain as to the detecting and warning capabilities against sophisticated cyberattacks.
4. **Alliances** are not discussed in publicly available documents. However, it is assumed that there has been some degree of international cooperation between the IDF and the US's cyber agencies, notably during the development of "Stuxnet."

2.4 Context/Analysis: Key Policy Principles

The Israeli conceptualization of cybersecurity has become increasingly holistic since the inception of its cybersecurity regime in 1998. As in various other developed countries, the initial civilian cybersecurity focus shifted away from CIP in the early 2000s to focus instead on technical superiority (2011). In 2015, the emphasis was then put on reorganizing the tasks of the intelligence community and the civil sector and set up a legal framework. The governmental resolutions of 2017 were the most recent efforts to centralize and reduce redundancies, thereby developing a robust and resilient cyber ecosystem. In this ecosystem, the government has put significant efforts into coordinating governmental, military, and private industry stakeholders. However, while there is an institutional separation of military and civilian cybersecurity and cyberdefense, tasks and information are often shared informally across organizations and agencies.

Concerning other national cyber strategies across the globe, two foci in Israel's strategy stand out. First, the military develops its cyberdefense and intelligence capabilities in response to explicitly mentioned enemies (Iran, Lebanon, Hezbollah, Hamas, Syria, ISIS, Palestinian Islamic Jihad, etc.) (Eizenkot, 2016, p. 4). Few other states shape their cyberdefense to confront specifically identified threat actors. To counter such threats, national agencies receive significant funding, closely cooperate, and exchange information. This is possible despite – or maybe because – no official cyberdefense strategy has been published. The security community increasingly embraces cyber tools as ways to achieve their goals. The IDF's strategy from 2015, the National Cybersecurity Strategy from 2017 and Ben Gurion's doctrinal principles of 1953, all mention the use of offensive capabilities. The intelligence services Mossad and Shin Bet take offensive actions as well. As will be explained later, these agencies often cooperate closely in applying these tools.

Second, the civilian cybersecurity strategy actively engages and supports the private sector to leverage its expertise while simultaneously strengthening the expanding Israeli high-tech industry. Investments in cybersecurity is seen as a potential for Israel's economy and innovation, as described by Prime Minister Netanyahu:

> *"I think that cybersecurity grows through cooperation, and cybersecurity as a business is tremendous. […] We spent an enormous amount on our military intelligence and Mossad and Shin Bet. An enormous amount. An enormous part of that is*

> *[…] being diverted to cybersecurity. […] We think there is a tremendous business opportunity in the never-ending quest of security"*(Netanyahu, 2018).

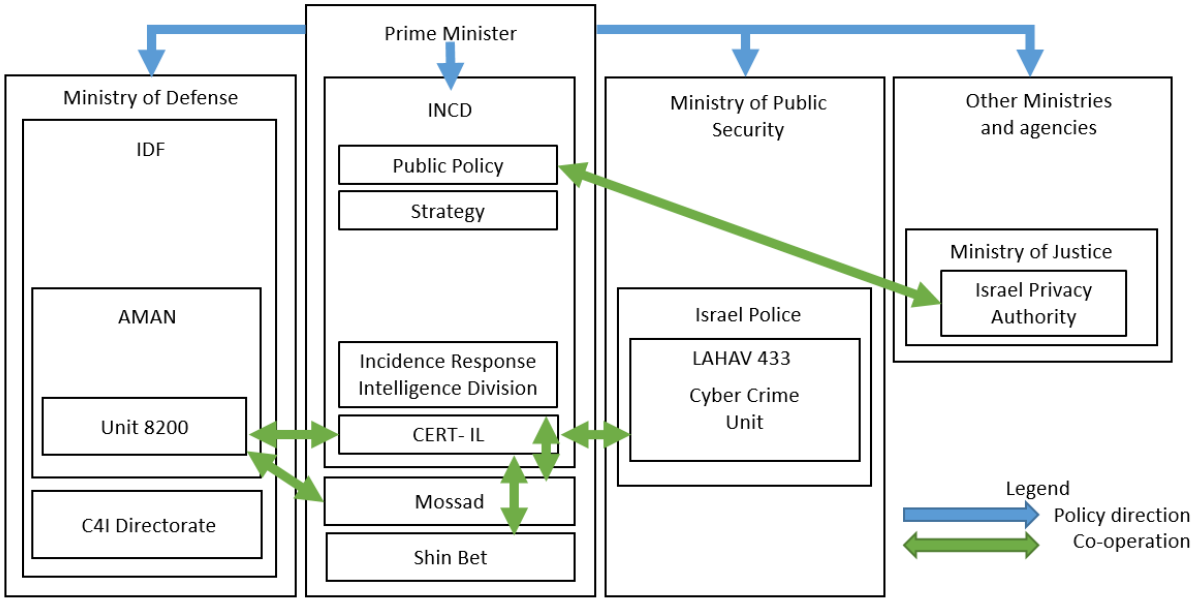
These investments contribute to expertise and knowledge creation, which bolster Israel's status as a technology-driven "start-up nation." The downside being that spread out expertise – in the private and public sectors – requires greater coordination to contribute to national security effectively. Creating the INCD is the most significant step towards the improvement of expertise, a stable legal framework, centralization of discretionary power, and clear ways of communication. By putting these efforts into the INCD and its coordination of various actors, the INCD leverages the expertise in both the public and the private sector to stabilize and secure the Israeli cyberspace.

3 Current Public Cybersecurity Structures and Initiatives

3.1 Overview of National Organization Framework

Diagram 3 provides an overview of the Israeli cybersecurity organization framework on a national level. Cooperation and policy direction between the IDF, INCD, Shin Bet, critical infrastructures, and other government ministries are often classified. As new cyber law is still being reviewed[3], there are no official policy directions and cooperation (Ginsburg, 2015; Rojkes Dombe, 2017). The directions in this diagram are thus not based on official declarations. This lack of official policy, however, allow the actors to (co)operate with a certain degree of flexibility. For example, if CERT-IL handles the case of a computer that is a threat for more networks, it usually relies on the company's cooperation. However, if the latter does not cooperate, CERT-IL can cooperate relatively freely with different institutions – e.g. Israel's Police or Shin Bet – to address the issue. These security institutions can notably use their authority to force the company to comply.

Diagram 3. Oversight Diagram



3.2 National Cybersecurity Structures and Initiatives: Organization, Mandate, Legal Aspects, and Operational capabilities

3.2.1 Israel National Cyber Directorate (INCD)

The INCD constitutes the core of the civilian cybersecurity architecture and is the result of the 2018 merger of the NCSA and the INCB. As such, it reports directly to the Prime Minister's Office giving it the option to escalate matters to the Prime Minister and thus indirectly taping into this position's policy direction. It is tasked with the following objectives (Adamsky, 2017, p. 120; Unna, 2018):

- Strategic policy planning to improve Israel's cyber robustness against risks by supporting critical infrastructures and imposing regulations.
- National-level implementation and regulation of the national cyber strategy (improving robustness, resilience and defense, which includes CERT-IL and CIP).
- Facilitation of international cooperation as well as formulation of legal framework for cyber activities (domestically and internationally).
- Comprehensive management of national defense campaigns (during peace time).
- Improve resilience in collaboration with the Israeli Police and Ministry of Justice.
- Support Shin Bet, IDF, Mossad, Israel Police and the Ministry of Justice in strengthening civilian cyberdefense.

[3] The Prime Minister's Office released a draft of the *Cyber Defense and National Cyber Directorate Bill* in June 2018, but due to the year-and-a-half-long political stalemate, followed by the corona crisis, the legislative efforts have not advanced beyond the draft stage.

Even though on paper, the INCD is the central and most powerful agency, cooperation with other agencies is often challenging. Most importantly, core values and operational approaches between Shin Bet and the INCD differ significantly, leading to month-long turf wars over authority, especially regarding CIP (Ravid, 2014). Also, while the intelligence community focuses on the protection of Israel's security from domestic threats with important technical capabilities, it often regards privacy and legality as a secondary issue. The INCD, however, seeks to coordinate such efforts in a broader national context and points out the necessity of legality (Tabansky & Ben Israel, 2015, p. 60). For the INCD, relying on the technical expertise of other agencies (most notably, Shin Bet, Mossad, and Unit 8200) can prove to be a double-edged sword. On the one hand, by involving these agencies into its tasks, the INCD (or CERT-IL) can re-allocate resources to other priorities than the development of technical expertise in-house. On the other hand, it is prone to external influence, especially by Shin Bet (Ziv, 2018).

The growth of the INCD's budget and number of employees is to be expected. In 2019, the budget was estimated between 32 million and 64 million USD, doubling the budget of 2017. Staff was also projected to grow from 220 in 2017 to 250 employees in 2019 (Ziv, 2018). The most challenging issue the INCD will face in the future is the vague legal framework – currently under revision but in a legislative stalemate. Unchanged, it allows the Prime Minister to order exhaustive investigation and surveillance on whomever he wants - even political adversaries – with little to no oversight mechanisms (Kubovich, 2019).

3.2.2 Shin Bet & Mossad

Shin Bet[4] and Mossad operate alongside the Israeli law enforcement agencies and civilian cybersecurity. They share expertise and information but remain separate from the INCD due to their mandate as intelligence services. This is why no public information is available on their cybersecurity-related tasks, actions, operational capabilities, and cooperation links with other agencies.

Shin Bet is also involved in cyberdefense but with different responsibilities than the IDF. It is involved in protecting critical communication infrastructure. Its task of cyberdefense is relatively comprehensive, exemplified by the 2018 hack of now alternate Prime Minister Benny Gantz's cellphone by Iran (allegedly). The security community was worried Iran would meddle with the 2019 elections by doxing its content. It fell under Shin Bet's responsibility to mitigate the risk (Haaretz, 2019; Harkov, 2019).

3.2.3 Israel Police

With approximately 20 people working in the cybercrime unit – LAHAV 433 – of the Israel Police, it is the weakest actor of the Israeli security community. It does not have a significant impact on policy development.

3.3 National Cyberdefense Structures and Initiatives: Organization, Mandate, Legal Aspects, and Operational Capabilities

Various institutions help foster a robust cyberdefense (the third layer of Israel's cybersecurity strategy), many of which have overlapping areas of responsibility. Amongst the main ones, we find the IDF's Unit 8200 and C4I Directorate, Shin Bet, the INCD, and Mossad but also – to a lesser extent – the Israeli Police and the Ministry of Justice (Unna, 2018). The two IDF actors mentioned first are the most crucial for Israel's cyberdefense and are examined in more detail in the following sections.

3.3.1 Unit 8200

Unit 8200[5] – also known as Central Collection Unit of the Intelligence Corps or Israeli SIGINT National Unit (ISNU) – covers the offensive spectrum of military use of cyber capabilities. It is subordinate to the Military Intelligence Directorate (AMAN).

After "Flame" became public in 2012, the IDF admitted carrying out – by Unit 8200 – offensive cyber operations (Katz, 2012). Besides "Flame," Unit 8200 allegedly developed "Duqu" (Katz, 2012) as well as "Stuxnet" in collaboration with the US-National Security Agency (NSA) (Symantec, 2011). These operations revealed aspects of its mandate: sabotage of industrial facilities, espionage, and support of traditional military forces.[6] The unit attaches importance to operational flexibility: Its legal restrictions are relatively lax, it has an organizational culture that accepts or encourages unprecedented offensive actions[7], and it operates with substantial financial resources.[8] It has relatively strong

[4] The Shin Bet's mandate is internal security while the Mossad's is external and strategic intelligence.

[5] For more details on the unit 8200, see Cordey, S. (2019). *Trend Analysis: The Israeli Unit 8200 – An OSINT-based study*. Center for Security Studies (CSS), ETH Zürich.

[6] An example is "Operation Orchard": Before the air raid of the Israeli Air Force on a Syrian nuclear facility, Unit 8200 conducted SIGINT to locate the facility, and during the attack, rendered the antiaircraft defense malfunctioning leveraging electronic sabotage.

[7] Stuxnet is considered the "world's first true cyber-weapon" (Motherboard, 2016).

[8] Stuxnet included four Zero-Day vulnerabilities.

operational capabilities as well as close ties to its American counterpart NSA. Non-IDF intelligence (Mossad and Shin Bet) cooperate with Unit 8200. In Israel, an estimated 90[9] per cent of all intelligence material is collected by Unit 8200, resulting in involvement in all of Mossad's major operations (Behar, 2016).

Soldiers join the unit at 18 and leave after four years[10], creating challenges for training recruits[11] and replacing 20 per cent of the manpower every year (Rhysider, 2018). According to estimations, 5,000 soldiers are assigned to Unit 8200 (Behar, 2016). Furthermore, Unit 8200's effect on Israel's tech industry is worth explaining. Before joining the unit at the age of 17, promising students are selected based on their analytical capabilities. They serve for four years from the age of 18. During that time, they are given high responsibility and are subjected to pressure to be creative. According to some reports, this culture makes 8200 alumni more likely to launch successful start-ups or do well in established companies. Due to the mandatory reserve duty until the age of 50, the IDF can count on well-connected and experienced tech experts that are at its disposal if required.

3.3.2 C4I Directorate

The C4I Directorate's – also known as C4I Corps or Teleprocessing Corps – mandate is to protect the IDF's communication infrastructure and teleprocessing systems. Furthermore, it supports the development of "relevant technology" (Raska, 2015, p. 5). Organizationally, the C4I Directorate is subordinate to the Computer Services Directorate (aka *Atak*).

Recently, C4I's approach to cyberdefense has shifted towards an "active defense" one, which entails a range of deterring and preempting attacks (Gross, 2017). This development corresponds to Ben Gurion's 1953 doctrinal principles for state-defense, especially the call for a rapid and decisive victory, deterrence, qualitative superiority, and supreme early warning capabilities. The C4I Directorate established a center, which integrates both the computer division and the military intelligence forces (Siboni & Assaf, 2016, p. 58, citing Zelinger, 2013). However, it faces financial limitations, which resulted in a reduction of its leadership from four to three brigadier generals (IsraelDefense, 2017).

3.4 Context: Key Public Organizational Framework

One of the main advantages of the Israeli organizational structure is that it gives way to a close and well-connected cybersecurity ecosystem where fast, efficient, and informal information exchange can take place. Indeed, as most cyber experts start their careers as soldiers in Unit 8200, they tend to maintain a social network that creates strong links between the private and public sector, military, and intelligence community.

More generally, Israel's cybersecurity and cyberdefense structures have become increasingly centralized under the IDF and the INCD. This centralization provides advantages and improvements: Less redundancy, consolidation of expertise, and improved information exchange due to less decentralization. However, the consolidation of power into the Prime Minister's Office, combined with public acceptance of privacy violation in exchange for enhanced general security, as well as a divided Knesset, could lead to abuses of political and cyber power, anti-democratic actions, and human rights abuses (e.g. ethnically discriminating surveillance of solely Palestinian citizens or political adversaries (Solomon, 2018)).The current *Cyber Defense and National Cyber Directorate bill* draft is a good example of such tendencies and a lack of checks and balances. According to the said draft, the INCD would be allowed to confiscate equipment related to a cyberattack even without a court order. Also, it could monitor all internet traffic (Kubovich, 2019; Solomon, 2018).

Furthermore, the INCD's central position in the Prime Minister's Office should be seen in the context of historically and technically powerful – but competitive – intelligence agencies. Accordingly, three trends can be observed. Firstly, the INCD was intended to solve the issue of agency infighting (Adamsky, 2017, p. 115). Indeed, by incorporating technical expertise – through CERT-IL – as well as being the strategic lead of Israel's cybersecurity structure-development, the INCD is supposed to become the uncontested cyber-authority in Israel. Still, worries about the influence of other organizations – especially Shin Bet – arise. Secondly, the INCD fits the understanding of the comprehensive character of cyber issues across the ministries. By locating it in the Prime Minister's Office, it is not placed in one specific ministry and thereby generating expertise, responsibility, and power to set the agenda for cyber-issues for this ministry only. Thirdly, the INCD's position also indicates the high degree of prioritization

[9] As a caveat, most of the cited information (such as the number of soldiers) are from secondary sources and are thus unconfirmed.

[10] Soldiers, which serve in positions for which extensive training is required, conscription exceeds the mandatory three years.

[11] Funded by the IDF, some exceptional high school students pursue their university diploma in engineering first and join the army later. Their compulsory service is extended by three to five years (Tabansky & Ben Israel, 2015, p. 19).

of cybersecurity, and cyberdefense. For the Israeli government, dealing with cyber threats is one of the utmost national political and security priorities – for both the military and the civilian side.

In 2015, the then Chief of Staff Gadi Eizenkot announced the unification of all cyber elements in a single united entity – similarly to the US’s cyber command. Despite Eizenkot favoring reorganization, these plans were put on hold, and the existing organizational separation between C4I Directorate, intelligence agencies and Unit 8200 remains (IsraelDefense, 2017; Bob, 2018). Amid these reorganizations, one organizational concept that will remain is that the IDF will maintain small and isolated cyber-subdivisions, whose soldiers operate on a need-to-know basis, in order to facilitate the containment of leaks (Behar, 2016).

Another adaptation of Israeli cyberdefense to the volatile situation in the Middle East is its flexible organizational adaptability when the threat level rises. In peacetime, the INCD is in charge of managing national cyberdefense. During times of emergencies, the IDF coordinates offensive and defensive cyber campaigns on a national level (Adamsky, 2017, p. 120). The IDF's 2015 to 2017 plans for a unified cyber command show that it still is in a transforming phase regarding cyber issues. Most notably, cyberdefense (C4I) has taken a more offensive direction but stays separated from Military Intelligence (Unit 8200).

The debate about the conceptualization and the organization of the IDF’s cyberdefense will continue in the future. Questions of unified cyber capabilities, cooperation with civil agencies, and the perspective on the military use of cyber capabilities (supportive to traditional forces or a division in itself, similar to air, ground, and sea) will be the most pressing ones.

Assessments of financial limitations have unsatisfactory informative value since officially published data is sparse. For example, the INCD's budget continually increases, yet, it is unclear how many external resources are being used through cooperation with other agencies (Ziv, 2018). No data are available on Mossad's, Shin Bet's, Unit 8200's, or C4I's budget.

4 Cyberdefense Partnership Structures and Initiatives

4.1 Public-Private Cyberdefense Partnerships

Resolution 3611 (2011) ordered the INCB (today INCD) "to advance coordination and cooperation between governmental bodies, defense community, academia, industrial bodies, businesses and other bodies relevant to the cyber field" (Prime Minister's Office, 2011, p. 4). Today, these efforts bear fruits: Various platforms for cooperation allow diffusion of expertise across sectors. Tel Aviv University's Yuval Ne'eman workshop (established in 2002) and the Blavatnik Interdisciplinary Cyber Research Center (inaugurated in 2014), together with the INCB, marked the first cooperation of government and academia for cyber-related research. It is a platform for informal exchange with representatives from the private, public, academia, and military sectors (Tabansky & Ben Israel, 2015, pp. 27-28).

CyberSpark, the Israeli cyber innovation ecosystem in Beersheba – near the Ben Gurion University –, is Israel's most visible project for public-private cyberdefense partnership. The military (i.e. C4I Directorate and eventually Unit 8200) and government (i.e. CERT-IL) decided to relocate significant organs of their cyberdefense there. This project has attracted the private sector too: Among others, Oracle, Lockheed Martin, IBM, Dell, Deutsche Telekom, and PayPal have decided to become part of this ecosystem (CyberSpark, 2017; Nakashima & Booth, 2016; Tabansky & Ben Israel, 2015, p. 28). Even though such ecosystems are not official cyberdefense public-private partnerships, they improve cooperation.

Finally, an anonymous information exchange platform (i.e. CyberNet+) allows the IDF to cooperate with the private sector by profiting from and being provided with crucial information.

4.2 International Cyberdefense Partnerships

The INCB conducted "national and international exercises to improve the State of Israel's preparedness in cyberspace" and advanced "cooperation in the cyber field with parallel bodies abroad" (Prime Minister's Office, 2011, p. 4). Only a few results are publicly known. Israel is a non-NATO ally and has strong ties to the United States' military (Eizenkot, 2016, p. 5) and cyber agencies, most notably the NSA. In 2016, Israel and the US signed a cyberdefense declaration, which outlines real-time operational connectivity for both CERTs (Opall-Rome, 2016; Adamsky, 2017, p. 124). Another partnership was outlined in a memorandum of understanding between the US and the Israeli government on matters of homeland security (DHS, 2008).

At the "Cyber Week" conference in June 2019, the director of the INCD presented a list of 36 countries and 13 organizations and companies Israel established international cooperation with, but without specifying how they cooperate.

4.3 Cyberdefense Awareness Programs

Resolution 3611 also instructed the former INCB "to advance and increase public awareness to threats in cyberspace and the means of coping with them" (Prime Minister's Office, 2011, p. 4). One approach to achieve this has been to organize and fund – by the INCD or the Ministry of Foreign Affairs – conferences. Examples include "Cyber Week" or "Cybertech." Their goal is to discuss cyber issues and raise the awareness of cyber threats. Another approach has been to promote awareness and knowledge through the private sector (National Cyber Directorate, 2017, p. 10). Finally, the education programs described below help improve awareness across the Israeli society.

4.4 Cyberdefense Education and Training Programs

According to Government Resolution 3611, education is another responsibility of the former INCB (Prime Minister's Office, 2011, p. 4). Together with the IDF and the Ministry of Education, it has developed various programs targeted at young Israelis. Amongst these, there are two after-school cyber programs – i.e. *Magshimim* and *Nitzanei Magshimim* – that help form, identify, and recruit young talents. Indeed, 75 per cent of the students who finish one of these later serve in the IDF's cyber and intelligence units (Kfir, 2018). A third program – e.g. *Gvahim* – complements the pre-military cyber education by preparing students for a high school matriculation exam in cybersecurity, computer science, and math (Housen-Couriel, 2017, p. 16).

The IDF has also developed two tracks to educate their cyber soldiers. Some exceptional high school students earn an IDF-funded degree in engineering before they join the army but have to serve an additional three to five years (Tabansky & Ben Israel, 2015, p. 19). The other track –*Talpiot* – is a 40-months elite training program for outstanding high school students, run by the Defense R&D Directorate (ibid.). After their service, soldiers often successfully enter the private high-tech sector and gain further experience. Since they are part of IDF's reserve force until the age of 40 to 50, the army profits of this part of their education process as well (ibid., pp. 19-20).

5 Annexes

5.1 Annex 1: Policy Spectra

These sliding scales represent three policy spectra:

1. The extent to which policy development and management in cyberdefense and cybersecurity is centralized;
2. The extent to which these areas fall under civilian or military oversight and;
3. Whether or not the state under examination takes a defensive or offensive approach to cyberdefense.

A state's position on these sliding scales is derived from the analysis conducted in the snapshot. For example, if a state focuses its policy development and implementation responsibilities significantly on just a few entities or even a single entity, it is reasonable to conclude that the relevant state takes a more centralized approach to cybersecurity and cyberdefense. Similarly, if responsibility for these sectors lies within the defense ministry, there will be a greater degree of military rather than civilian oversight, and if offensive cyberdefense capabilities are explicitly referred to in policy literature, a state can reasonably be assumed to take an offensive stance on cyberdefense, even if specific capabilities or tools are not mentioned.

Centralization vs Decentralization of Leadership

Diagram 4: Spectrum of Centralization vs Decentralization of Policy Development and Management

Centralized control ----- X ---------- Decentralized control

Civilian vs defense posture and oversight

Diagram 5: Spectrum of Civilian-Defense Cybersecurity Posture and Oversight

Civilian oversight ---------- X ---------- Defense oversight

Offensive vs defensive capabilities

Diagram 6: Spectrum of Offensive vs Defensive Cyberdefense Capabilities

Offensive ---------X---------- Defensive

5.2 Annex 2: Key Definitions

Term	Definition
Cyberattack	The deliberate exploitation of computer systems, digitally dependent enterprises and networks to cause harm
Cyber incident	An occurrence that actually or potentially poses a threat to a computer, internet-connected device, or network – or data processed, stored, or transmitted on those systems – which may require a response action to mitigate the consequences
Cyber resilience	The overall ability of systems and organizations to withstand cyber events and, where harm is caused, recover from them
Cybersecurity	The protection of internet-connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorized access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so
Prime Minister's Office	It assists the Prime Minister in his or her work. It also coordinates inter-ministerial activities in various fields, according to the priorities determined by the Prime Minister and in accordance with government resolutions

5.3 Annex 3: Abbreviations

Abbreviations/Acronyms	English	Hebrew
C4I Directorate	Computer Service Directorate	n/a
CERT-IL	Israel National Cyber Event Readiness Team	מתאם
IDF	Israel Defense Forces	ל"צה
INCB	Israel National Cyber Bureau	הלשכה הלאומי הסייבר
INCD	Israel National Cyber Directorate	הלאומי הסייבר מערך
Magshimim, Nitzanei Magshimim & Gvahim	After-school programs for pupils	מגשימים
NCSA	National Cyber Security Authority	הסייבר להגנת הלאומית הרשות
NISA (or Re'em)	National Information Security Authority	הסייבר להגנת הלאומית הרשות
NSA	National Security Agency	
Shin Bet	Israel's internal security service, also known as Israel Security Agency (ISA) or Shabak	הכללי הביטחון שירות
Talpiot	IDF training program for exceptional high school students	תלפיות תוכנית

6 Bibliography

Adamsky Dmitry, "The Israeli Odyssey towards its National Cyber Security Strategy", *The Washington Quarterly.* 40:2 (2017), pp. 113-127. https://www.tandfonline.com/doi/abs/10.1080/01636 60X.2017.1328928

ADM, "PM signs cyber security MoU with Israel," *Australia Defence Magazine,* 01.11.2017. https://www.australiandefence.com.au/defence/cyber -space/pm-signs-cyber-security-mou-with-israel

Baezner Marie, & Robin Patrice, *Hotspot Analysis: Stuxnet* (Zürich: CSS/ETH, 2017).

Behar Richard, "Inside Israel's Secret Startup Machine," *Forbes,* 11.05.2016. https://www.forbes.com/sites/richardbehar/2016/05/ 11/inside-israels-secret-startup-machine/

Ben Gurion David, *Ben Gurion's report to the Cabinet, 18 October 1953* (1953).

Bob Yonah Jeremy, "Eisenkot: Someday the IDF will be under one cyber command," *The Jerusalem Post,* 24.10.2018. https://www.jpost.com/Israel-News/Eisenkot-Someday-the-IDF-will-be-under-one-cyber-command-570230

Breznitz Dan, "The military as a public space: the role of the IDF in the Israeli Software Innovation System", *Samuel Neaman Institute for Advanced Studies in Science and Technology*, pp. 130-48.

Brom Sholom, "Operation Desert Fox: Results and Ramifications" *Strategic Assessment*, 2:1 (1999), pp. 13-18. https://www.inss.org.il/publication/operation-desert-fox-results-and-ramifications/

Congress.gov, "H.R.4860 - United States - Israel Cybersecurity Cooperation Act," *US Congress,* 2016. https://www.congress.gov/bill/114th-congress/house-bill/4860?r=202

Cornish, & Kavanagh, "Geneva Dialogue on Responsible Behaviour in Cyberspace. Phase 1 Report," *Geneva Dialogue on Responsible Behaviour in cyberspace*, 2019. https://genevadialogue.ch/wp-content/uploads/Geneva-Dialogue-on-Responsible-Behaviour-Final-Report.pdf

Council of Europe, *Charts of signatures and ratifications of Treaty 185*, coe.int, 2019. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=ly6zAR21

CyberSpark, *CyberSpark Ecosystem*, facebook.com, 2017. https://www.facebook.com/cyberspark.org.il/videos/vb.1419456708084868/1420977634599442/?type=2&theater

DHS, "Agreement between the government of the United States of America and the government of the State of Israel on cooperation in science and technology for homeland security matters," *DHS*, 2008. https://www.dhs.gov/xlibrary/assets/agreement_us_israel_sciencetech_cooperation_2008-05-29.pdf

Efrat Kalanit, "The direct and indirect impact of culture on innovation," *Technovation*, 34:1 (2014), pp. 12-20. https://www.sciencedirect.com/science/article/abs/pii/S0166497213001028

Eizenkot, Gadi, "Deterring Terror. How Israel Confronts the Next Generation of Threats.", 2016. Translated by Rosenberg, S. Belfer Center Special Report. https://www.belfercenter.org/sites/default/files/legacy/files/IDF%20doctrine%20translation%20-%20web%20final2.pdf

Freilich Charles, "Israel's National Security Policy. In: Hazan Reuven, Dowty Alan, Hofnung Menachen, & Rahat Gideon, *The Oxford Handbook of Israeli Politics and Society* (Oxford: 2018). https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780190675585.001.0001/oxfordhb-9780190675585-e-25?print=pdf

Getz Daphne, & Tadmor Zehev, *Israel in UNESCO Science Report Towards 2030* (Paris: United Nations Educational Scientific and Cultural Organization, 2015), pp. 408-429. https://en.unesco.org/sites/default/files/usr15_israel.pdf

gov.il, *1.* מתן *2*איחוד יחידות מערך הסייבר הלאומי . הוספת *3*פטור ממכרז למשרת ראש מערך הסייבר הלאומי . לחוק *23*משרת ראש מערך הסייבר הלאומי לתוספת לפי סעיף קביעת שכר ותנאי שירות של ראש *4*שירות המדינה (מינויים) . מערך הסייבר הלאומי, 2017. https://www.gov.il/he/departments/policies/dec_3270_2017

gov.il, *Israel National Cyber Directorate*, gov.il , 2018. https://www.gov.il/en/departments/about/newabout

Groll Ellias, "The Future Is Here, and It Features Hackers Getting Bombed," *Foreign Policy*, 06.02.2019. https://foreignpolicy.com/2019/05/06/the-future-is-here-and-it-features-hackers-getting-bombed/

Gross, Judah Ari, "Army beefs up cyber-defense unit as it gives up idea of unified cyber command," *The Times of Israel*, 14.02.2017 https://www.timesofisrael.com/army-beefs-up-cyber-defense-unit-as-it-gives-up-idea-of-unified-cyber-command/

Haaretz, "Israel Says Iran Hacked Ex-general Gantz's Phone Ahead of Election," *Haartez,* 14.03.2019. https://www.haaretz.com/israel-news/elections/benny-gantz-s-cellphone-hacked-by-iranian-intelligence-1.7022269

IsraelDefense, "IDF Scraps Plans for a Unified Cyber Command," *IsraelDefense*, 15.05.2017. https://www.israeldefense.co.il/en/node/29613

Harkov Lahav, "Politics: The cybersecurity election," *The Jerusalem Post*, 04.04.2019. https://www.jpost.com/Israel-Elections/Politics-The-cybersecurity-election-585802

Housen-Couriel Deborah, "National Cyber Security Organisation: ISRAEL,"*CCDCOE*, 2017. https://www.ccdcoe.org/uploads/2018/10/IL_NCSO_final.pdf

IDF, *CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work. HamasCyberHQ.exe has been removed,* Twitter.com, 05.02.2019. https://twitter.com/IDF/status/1125066395010699264

Katz, Yaakov, "IDF admits to using cyber space to attack enemies," *The Jerusalem Post,* 03.06.2012. https://www.jpost.com/Defense/IDF-admits-to-using-cyber-space-to-attack-enemies

Kfir Issac, "Learning from Israel's cyber playbook," *Asia & the Pacific Policy Society*, 2018. https://www.policyforum.net/learning-israels-cyber-playbook/

Kubovich Yaniv, "Hamas Cyber Ops Spied on Hundreds of Israeli Soldiers Using Fake World Cup, Dating Apps," *Haartez*, 03.07.2018. https://www.haaretz.com/israel-news/hamas-cyber-ops-spied-on-israeli-soldiers-using-fake-world-cup-app-1.6241773

Kubovich Yaniv, "Cyber Bill Would Give Netanyahu Unsupervised Powers, Experts Warn", *Haartez,* 19.03.2019. https://www.haaretz.com/israel-news/.premium-cyber-bill-would-give-israeli-prime-minister-unsupervised-powers-experts-warn-1.7040402

Lappin Yaakov, "Iran attempted large-scale cyber-attack on Israel, senior security source says," *The Jerusalem Post,* 17.08.2014. https://www.jpost.com/Arab-Israeli-Conflict/Iran-attempted-large-scale-cyber-attack-on-Israel-senior-security-source-says-371339

Franceschi-Bicchierai Lorenzo, "The History of Stuxnet: The World's First True Cyberweapon," *Motherboard*, 09.08.2016. https://www.vice.com/en_us/article/ezp58m/the-history-of-stuxnet-the-worlds-first-true-cyberweapon-5886b74d80d84e45e7bd22ee

Nakashima & Booth, "How Israel is turning part of the Negev Desert into a cyber-city," *The Washington Post*, 14.05.2016. https://www.washingtonpost.com/gdpr-consent/?next_url=https%3a%2f%2fwww.washingtonpost.com%2fworld%2fnational-security%2fhow-israel-is-turning-part-of-the-negev-desert-into-a-cyber-city%2f2016%2f05%2f14%2ff44ea8e4-0d58-11e6-bfa1-4efa856caf2a_story.html%3futm_term%3d.377658480264&utm_term=.377658480264

INCD, "Israel National Cyber Security Strategy in Brief," *Prime Minister Office*, 2017. https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf

Netanyahu Benjamin, *PM Netanyahu Addresses CyberWeek 2018 Cybersecurity Conference*, youtube.com, 20.06.2018. https://www.youtube.com/watch?v=0HXEbGamgcQ

OECD, "Gross domestic product (GDP)," *OECD,* 2019a. https://data.oecd.org/gdp/gross-domestic-product-gdp.html

OECD, "Gross domestic spending on R&D," *OECD, 2019b.* https://data.oecd.org/rd/gross-domestic-spending-on-r-d.html

Opall-Rome Barbara, "US-Israel sign cyberdefense declaration," *Federal Times,* 22.06.2016. https://www.federaltimes.com/2016/06/22/us-israel-sign-cyber-defense-declaration/

Prime Minister's Office, "Advancing National Cyberspace Capabilities," *Prime Minister Office,* 2011. http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf

Prime Minister's Office, "Government Resolution No. 2443 of February 15, 2015," *Prime Minister's Office*, 2015a. https://ccdcoe.org/sites/default/files/documents/Government%20Resolution%20No%202443%20-%20Advancing%20National%20Regulation%20and%20Governmental%20Leadership%20in%20Cyber%20Security.pdf

Prime Minister's Office, "Government Resolution No. 2444 of February 15, 2015," *Prime Minster Office,* 2015b. https://ccdcoe.org/sites/default/files/documents/Government%20Resolution%20No%202444%20-%20Advancing%20the%20National%20Preparedness%20for%20Cyber%20Security.pdf

Raska, M. "Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy," *S. Rajaratnam School of International Studies, Nanyang Technological University*, 2016.

Ravid Barak, "Israeli Security Agencies in Turf Battle Over Cyber War; Netanyahu to Decide," *Haartez,* 14.09.2014. https://www.haaretz.com/israeli-agencies-in-cyber-turf-battle-1.5300816

Rhysider, *Ep 28: Unit 8200*, darknetdiaries.com, 2018. https://darknetdiaries.com/episode/28/

Rojkes Dombe Ami, "The IDF C4I Directorate is Preparing for the Next War," *Israel Defense,* 07.12.2017. https://www.israeldefense.co.il/en/node/32116

Senor Dan & Singer Saul, *Start-up nation: The story of Israel's economic miracle* (London: Random House Digital, Inc., 2011)

Shamah David, "Qatari tech helps Hamas in tunnels, rockets: Expert," *The Times of Israel*, 31.07.2014. https://www.timesofisrael.com/qatari-tech-helps-hamas-in-tunnels-rockets-expert/

Shtokhamer Lavy, *CERT-IL Workflow & Financial CERT Case Study*, video-tau.ac, 2018. https://video.tau.ac.il/events/index.php?option=com_k2&view=item&id=8916:cert-il-workflow&Itemid=559

Siboni Gabi & Assaf Ofer, *Guidelines for a national cyber strategy* (Tel Aviv: Institute for National Security Studies, 2016). https://www.inss.org.il/wp-content/uploads/systemfiles/INSS%20Memorandum%20153%20-%20Guidelines%20for%20a%20National%20Cyber%20Strategy.pdf

Siboni Gabi & Sivan-Sevilla Ido Sivan, "Israeli Cyberspace Regulation: A Conceptual Framework, Inherent Challenges, and Normative Recommendations," *Cyber, Intelligence, and Security*, 1:1 (2017). pp. 83-102.

Solomon Shoshanna, "Why is Israel's new proposed cybersecurity law raising hackles?," *The Times of Israel,* 25.06.2018. https://www.timesofisrael.com/why-is-israels-new-proposed-cybersecurity-law-raising-hackles/

Solomon Shoshanna, "Bulgaria, Israel mull cybersecurity cooperation," *Times of Israel*, 22.03.2018. https://www.timesofisrael.com/bulgaria-israel-mull-cybersecurity-cooperation/

Start-up Nation Central, "Discover the secrets of cybersecurity," *Start-up Nation Central.* https://www.startupnationcentral.org/sector/cybersecurity/

Swed Ori & Butler John Sibley, "Military capital in the Israeli Hi-tech industry," *Armed Forces & Society*, 41:1 (2015), pp. 123-141.

Symantec, "W32.Duqu – The precursor to the next Stuxnet," *Symantec,* 2011. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

Tabansky Lior, "Critical infrastructure protection from cyber threats," *Mil Strategy Affair*, 3:2 (2011), pp.61–78.

Tabansky Lior & Ben Israel Isaac, *Cybersecurity in Israel* (Cham: Springer International Publishing, 2015).

Tor Uri, "Cumulative Deterrence as a New Paradigm for Cyber Deterrence," *Journal of Strategic Studies*, 40:1-2 (2017), pp. 92-117.

Tsipori Tali, "Israeli cybersecurity grabs 8% global market share," *Globes*, 04.04.2016. https://en.globes.co.il/en/article-israeli-cyber-industry-hits-the-big-time-1001114669

United Nations General Assembly, "Advancing responsible State behaviour in cyberspace in the context of international security," *United Nations* 2018. https://undocs.org/A/C.1/73/L.37

Unna Yigal, *Cyber Israel – The New National Cyber Directorate,* video.tau.com, 2018. *https://video.tau.ac.il/events/index.php?option=com_k2&view=item&id=8911:cyber-israel&Itemid=559&highlight=WyJ5aWdhbCIsInVubmEiLCJ5aWdhbCB1bm5hIl0=*

Zack Hudi, *The Pillars of State-Level Cyberdefense,* video.tau.com, 2018. https://video.tau.ac.il/events/index.php?option=com_k2&view=item&id=8912:the-pillars-of-state&Itemid=559

Zelinger, הסייבר, זירת הלחימה החדשה של צה"ל - עבשיו הסרט, *Haartez,* 2013. http://www.haaretz.co.il/news/politics/1.1946156

Ziv Amitai, "'A Shin Bet Puppet' // What Went Wrong With Israel's Cybersecurity Agency," *Haartez,* 29.08.2018. https://www.haaretz.com/israel-news/business/.premium-cybersecurity-agency-drops-role-of-protecting-business-1.6429506

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.