ETH zürich

ETH Library

# The Israeli Unit 8200 – An OSINT-based study

## Trend Analysis

**Report**

**Author(s):**
Cordey, Sean

**Publication date:**
2019-12-31

**Permanent link:**
https://doi.org/https://doi.org/10.3929/ethz-b-000389135

**Rights / license:**
In Copyright - Non-Commercial Use Permitted

**Originally published in:**
CSS Cyberdefense Trend Analyses

This page was generated automatically upon download from the ETH Zurich Research Collection.
For more information, please consult the Terms of use.

**CSS** CYBER DEFENSE PROJECT

# Trend Analysis

# The Israeli Unit 8200
# An OSINT-based study

Zürich, December 2019

Risk and Resilience Team
Center for Security Studies (CSS), ETH Zürich

CSS
ETH Zurich

ETH zürich

Author: Sean Cordey

© 2019 Center for Security Studies (CSS), ETH Zurich
Contact:
Center for Security Studies
Haldeneggsteig 4
ETH Zurich
CH-8092 Zurich
Switzerland
Tel.: +41-44-632 40 25
*css.info@sipo.gess.ethz.ch*
*www.css.ethz.ch*

Analysis prepared by: Center for Security Studies (CSS), ETH Zurich

ETH-CSS project management: Tim Prior, Head of the Risk and Resilience Research Group, Myriam Dunn Cavelty, Deputy Head for Research and Teaching; Andreas Wenger, Director of the CSS

Disclaimer: The opinions presented in this study exclusively reflect the authors' views.

Please cite as: Cordey, S. (2019). *Trend Analysis: The Israeli Unit 8200 – An OSINT-based study*. Center for Security Studies (CSS), ETH Zürich.

# Table of Contents


**1 Introduction 4**

**2 Historical Background 5**
2.1 Pre-independence intelligence units 5
2.2 Post-independence unit: former capabilities, missions, mandate and techniques 5
2.3 The Yom Kippur War and its consequences 6

**3 Operational Background 8**
3.1 Unit mandate, activities and capabilities 8
3.2 Attributed and alleged operations 8
3.3 International efforts and cooperation 9

**4 Organizational and Cultural Background 10**
4.1 Organizational structure 10
Structure and sub-units 10
Infrastructure 11
4.2 Selection and training process 12
Attractiveness and motivation 12
Screening process 12
Selection process 13
Training process 13
Service, reserve and alumni 14
4.3 Internal culture 14

**5 Discussion and Analysis 16**
5.1 Strengths 16
5.2 Weaknesses 17

**6 Conclusion and Recommendations 18**

**7 Glossary 20**

**8 Abbreviations 20**

**9 Bibliography 21**

# Executive Summary


**Objective**

Since Dan Senor and Saul Singer first broke the silence in their 2009 book "Start-Up Nation", much ink has been spilled about the now (in)famous Israeli Unit 8200. Indeed, a plethora of articles and literature shed light on one aspect or another of the mystery that is Unit 8200. But the disparity of the available information makes any comprehensive analysis of the Unit very difficult. This is notably the case for any interested policymakers who wish to understand, replicate or get inspiration from this renowned Unit.

Accordingly, the purpose of this study is to try to make sense of this plethora of scattered information and to synthetize it to the best extent possible in order to clarify the lines between myth, propaganda and reality. More specifically, this Trend Analysis (TA) has two underlining goals. First, it reviews the historical, operational, organizational and cultural background of the Unit in order to make it easier for policymakers to understand what it actually is and what it does. Second, this TA provides a deeper assessment of the Unit by discussing its core strengths and weaknesses. This will allow policymakers to understand the underlying dynamics of the Unit's success and functioning while also identifying key best practices and developing recommendations for applying the insights gained to their specific circumstances.

**Results**

In terms of findings, the origins of Unit 8200 can be traced back to the pre-independence intelligence unit Shin Mem 2. After independence, the Israel Defense Force (IDF) consolidated that unit with several other intelligence and signal gathering groups, setting up an electronic warfare unit called Unit 515 (and later on 848), which had a very small budget in relative terms. The turning point for the Unit was the 1973 Yom Kippur War and the intelligence failure it highlighted. This led to a complete overhaul of the Unit's structure (then renamed 8200) and left an indelible mark on its culture.

Regarding its organization and structure, the Unit is the largest unit in the IDF, comprising several thousand soldiers (at least 5,000 on active duty) separated into various smaller units and operating numerous bases as well as other mobile SIGINT modules. In order to reach the required quality level in terms of manpower and capabilities, the Unit has set up a highly selective and competitive screening, selection and training process for new recruits, who are required to complete their mandatory military service. Screening starts during high school already in the form of state and private programs for young talents. Meanwhile, selection tests comprise a psychometric test, rigorous interviews, and an education/skills test. The education and training that follows is as intense as it is comprehensive, covering everything from communication to electrical engineering and Arabic language skills. In terms of profile, the emphasis lies not only on technical proficiency but also, and most importantly, on the capacity to learn quickly and think critically. Consequently, the prevalent culture in the Unit is one of flexible thinking, resourcefulness, risk-taking, rapid adaptation, teamwork and a flat hierarchy.

Serving primarily as the signal intelligence and decryption unit, Unit 8200 is very active and prolific. It has notably conducted a number of intelligence, offensive and defensive operations across cyberspace. The most widely known among these are Stuxnet, Operation Orchard (2007), Operation Full Disclosure (2014) and the Ogero Incident (2017). Other unattributed but suspected campaigns include Flame, Duqu, Gauss, miniFlame and Duqu 2.0. Moreover, the Unit works in close cooperation with the American NSA.

In addition to intelligence and security implications, the Unit's modus operandi has further, more general implications for the high-tech sector in Israel. Indeed, the Unit is considered by many as an incubator for future very successful cybersecurity start-ups, technology venture capitalists, and cybersecurity experts. This reputation, alongside with patriotism, is a main motivation for young recruits to join the Unit. Compared with traditional civilian and private incubators, the Unit's military culture, missions and network allow the development of specific leadership, technical and entrepreneurial skills at a young age and foster a high level of trust between alumni.

This report identifies the Unit's core strengths as being its human and financial resources, institutional capabilities and know-how, internal culture, branding, selection process and close cooperation with the private sector. Meanwhile, it suffers from various political controversies, some bureaucratic encroachment, risk of elitist tendencies, difficulties with the post-service transition of its members, and increased political scrutiny. Based on a review of these strengths and challenges, this report suggest the following generalizable policy recommendations for successful cyber programs: 1) provide adequate human and financial resources; 2) promote regular and continuous transmission of know-how and experience; 3) foster an internal culture of entrepreneurship and innovation; 4) develop and nurture ties with the private sector; 5) enhance the general and professional attractivity of the program for both recruits and future employers; 6) develop public awareness of the program.

# 1 Introduction

In today's high-tech and cybersecurity world, Israel is often synonymous with innovation platforms, successful start-ups and strong relations between the private sector and the military. The reasons and dynamics behind this technological and commercial success have been extensively studied over the years. Amongst these studies, one book in particular stands out, namely Dan Senor's and Saul Singer's 2009 book, "Start-Up Nation: The Story of Israel's Economic Miracle". While their thorough analysis of Israel's technological success – which the authors base on Israel's culture, diversity and mandatory military service as well as the existential threat that is felt by most Israelis (Senor and Singer, 2009) – is interesting, the book stands out as the first piece of literature to publicly break the silence over a military unit which had until then remained extremely secret: the now (in)famous Unit 8200.

Since then, much ink has been spilled about the Unit, notably about its very prolific and mediatized alumni. Accordingly, the literature on Unit 8200 can be divided into two separate strands. The first, more academic strand studies Israel's cyberdefense policy, structure, capabilities and operations in general, with some more specific examination of the role and place of Unit 8200. The second strand, meanwhile, is largely comprised of media articles published in specialized (e.g. regional, intelligence, business, defense) or mainstream journals along with some academic papers, notably by Rousseau (2007). These articles are mostly in the forms of interviews with former Unit members, who discuss some anecdotes, processes and lessons learned from their time there. Other articles cover investigations of the Unit's alleged bases, missions and capabilities as well as scandals surrounding it.

The purpose of this study is thus to try to make sense of this large volume of scattered information and to synthetize it to the best extent possible in order to shed light on the myth, propaganda and reality of Unit 8200. It therefore has two underlining goals: First, it wants to make it easier for policymakers to understand what this Unit actually is and what it does. Second, this TA enables policymakers to understand the underlying dynamics of the Unit's success and functioning to provide a sound basis from which to identify relevant best practices.

In order to do so, this study thus successively focuses on various aspects of the Israeli Defense Force's (IDF) Unit 8200. Its first part examines the Unit's historical background and evolution since Israeli independence. Its second part discusses the Unit's operational background, notably its mandate, capabilities and alleged operations. The third part focuses on Unit's organizational background, in particular its structure, infrastructure, and selection and education processes before looking into its culture. The considerations in the last part synthesize the findings from the earlier sections and identify both strengths and weaknesses of Unit 8200. On this basis, the report then concludes by suggesting and discussing a set of generalizable recommendations for other, similar organizations.

**Disclaimer**

The data for this report was drawn from available open-source material (OSINT). Such data can be of great value – particularly when it enables cross-referencing – but it can also be problematic, as its complete veracity can never be guaranteed. Given the elusive nature of the Unit – famous but nonetheless secretive –a comprehensive overview of its history, organization, operations and capabilities is very challenging to achieve, and numerous details about its origin and involvement in internal and external affairs remain unclear.

# 2 Historical Background

## 2.1 Pre-independence intelligence units

The origins of Unit 8200 can be traced back to the activities and legacies of a number of pre-independence intelligence and signal gathering groups, most of which operated during the British mandate and were very active during the Arab revolt of 1935–39 and until Israeli independence in 1948.

The oldest of these modern Jewish intelligence groups is **Netzah Yisrael Lo Yeshaker** (NILI), meaning "The Eternal One of Israel will not lie". This spy ring served as a clandestine pro-British agency collecting intelligence on the Ottomans (e.g. troop formations and movements) and the region (e.g. weather patterns, invasion routes) for the invading forces (Florence, 2007; Goldstone, 2007; in Rousseau, 2017).

Following the partition of the caliphate and the establishment of Mandatory Palestine (1920-1948), the **Haganah** or "defense" was formed as an underground militia protecting Jews against attacks by Arab militias. In 1929, members of the Haganah created the **Shin Mem 2** unit, which would become the first signal intelligence[1] unit (aka. SIGINT) that oversaw radio intelligence and monitored enemy signals traffic (Black and Morris, 1991; Kidon, 2008). Over the years, and notably following the bloody quelling of the 1929 Arab riots and the Buraq Uprising, the Haganah became an increasingly central, mature and professional organization (Friedman, 1997; in Rousseau, 2017) that cooperated with British intelligence services to organize preemptive night raids on Arab forces (Shindler, 2008; in Rousseau, 2017).
During that time, the Haganah established several covert intelligence units, notably the **Mossad Le' Aliyah Beth (Mossad)** or "Institution for Immigration B", which was in charge of organizing illegal Jewish immigration from all over Europe into Palestine. (Schindler, 2008; in Rousseau, 2017). Another one was **Sheruth Yedioth (Shai)** or "the Information Service", which served as the intelligence and counter-espionage arm of the Haganah and can be considered the forebear of the Military Intelligence Directorate of the IDF, which would later include the precursors of Unit 8200 (Kahana, 2006).

In the wake of the Second World War, persistently anti-Zionist British policies fostered an open, organized struggle against British Mandatory rule. In October 1945, the Haganah allied with two other paramilitary organizations, Irgun Zevai Le'umi (Etzel) and Lohamei Herut Yisrael (Lehi), to form *The Unified Jewish Resistance Movement* or *United Resistance Movement*. The same groups would later form *Tsahal* or the Israeli Defense Force (IDF) (Perman, 2005). Subsequently, a succession of events including the 1946 attack against the British administrative headquarters for Palestine by Irgun Zevai Le'umi, the creation of a UN Special Committee on Palestine, the rejection of UN General Assembly Resolution 181, the collapse of the British mandate, and the civil war that followed, among others, led David Ben-Gurion to declare the establishment of an independent State of Israel on May 14th, 1948. Later that day, armies from Egypt, Syria, the Emirate of Transjordan, Iraq, and Lebanon joined together and invaded the newly established state of Israel in what would be the first of several Arab-Israeli wars (Shindler, 2008; in Rousseau, 2017). It is said that Israel was able to defeat the Arab forces partly due to the vast intelligence networks the Haganah had developed throughout the previous decades (Perman, 2005).

## 2.2 Post-independence unit: former capabilities, missions, mandate and techniques

In the years following its independence and the first Arab-Israeli war, Israel consolidated and formalized its state structures, notably its intelligence agency tryptic: the *Shin Bet* or "Security Service", also known as the Israel Security Agency (ISA); the *HaMossad leModiʿin uleTafkidim Meyuḥadim* or "Institute for Intelligence and Special Operations"; and the *Agaf HaModi'in lit* or "Intelligence Section", also known as the Military Intelligence Directorate or AMAN.[2]

The latter of these set up an electronic warfare unit called Unit 515 (renamed Unit 848 in 1968) or Central Warning Unit in a villa, which had formerly belonged to an Arab sheik in the old port town of Jaffa (Kahana, 2006). The group was given the codename "Rabbit" and had two main sections: SIGINT, which tried to intercept enemy communications, and Deciphering Intelligence in charge of breaking codes and making sense of the data gathered (Kahana, 2006). It is interesting to note that this technological ability of the latter group was mostly developed by early Israeli computer engineers, some of whom had emigrated from the Soviet Union (Shamir, 2005).

In relative terms, the Unit was not only small but also operated with a very limited budget compared with its large modern-day counterpart. In 1950, the Unit was allocated a US$15,000 budget and an additional US$110,000 for initial electronic hardware – mostly American surplus stock (Perman, 2005). In today's currency, this would be equivalent to approximatively US$1.25 million, which is very little according to both modern and earlier standards. As a result, the Unit developed most of its own hardware and software in-house with few people and limited resources, both due to its low budget and to maintain secrecy around its

[1] Technical terms are explained in a glossary in Section 7.

[2] Abbreviations are listed in section 8.

intelligence capabilities. This trend has persisted until modern times, albeit with larger budgets (Perman, 2005).

Overall, in the early years of its existence, Unit 515 faced a number of particular restraints its Western counterparts were not subject to, namely a lack of technical experience, technological institutions, funds, and manpower (Rousseau, 2017). However, in order to compensate, members of the Unit resorted to "crude, albeit effective, techniques to pick up and monitor enemy communications" (Rousseau, 2017). For instance, they strung up an antenna made of metal wire between two poles and connected it to an old Hallicrafter's S-38, a popular civilian radio in the 1930's and 40's. Later on, the Unit would develop more sophisticated monitoring systems mostly based on stolen BBC plans (Perman, 2005).

The Unit's resourcefulness and combativeness came from necessity and urgency in the context of continuous Arab guerilla attacks and aggressions throughout the 50's and 60's. Accordingly, the Unit – and the army at large – was constantly striving to ensure and preserve its competitive edge over its enemies, whatever the circumstances it faced. This mindset is best described in Hebrew as *davka*, which roughly translates into English as "'despite' with a 'rub their nose in it' twist" (Rousseau, 2017; Senor and Singer, 2009). According to Perman, the Unit has embodied this concept since its infancy (Perman, 2005).

In 1954, the Unit moved from Jaffa to its current base at the Glilot Junction (Kidon, 2008). By then, it had greatly expanded its range and had spread out its listening bases across Israel.

Over the years, the Unit continued to gain access to more and more advanced computing technology. For instance, the IDF's military R&D unit RAFAEL – aka Authority for the Development of Armaments – had, in 1956, developed one of the first analog computers in Israel. By 1958, the same unit had created a computer called Itzik, which allowed for large-scale simulations, and access to which was then (probably) granted to the Unit (Breznitz, 2002; in Rousseau, 2017). Two years later, the IDF bought a Philco computer from the US and created *Merkaz Mahshevim UMa'arahot Meida* or "The Center for Computers and Mechanized Records" (MAMRAM) (Breznitz, 2002; in Rousseau, 2017).

This new computing power was used by the Unit and the IDF at large during the 1967 Six-Day War in particular. With it, the Unit and the IDF were able to intercept and decipher Egyptian and Syrian air force communications, which allowed the smaller, less sophisticated Israeli air force to outmaneuver and control the airspace (Perman, 2005). The successful simultaneous defeat of Egyptian, Syrian, and Jordanian forces in such a short campaign, which substantially enlarged Israel's territory, gave the Israelis, the IDF and the intelligence a sense of invincibility (Senor and Singer, 2009; in Rousseau, 2017).

Following the Six-Day War, the IDFs SIGINT Unit (now 848) was allocated substantial budgets to improve its capability to collect information, particularly on Syria and Egypt (Kahana, 2006). Several SIGINT centers were built, notably at Tel Avital in the Golan Heights, on Mount Hermon and in Um-Hashiba in the Sinai Desert, to collect evidence and communications intelligence in order to provide an early warning should a war be launched (Kahana, 2006).

## 2.3 The Yom Kippur War and its consequences

The Unit's turning point came along with what many regard as one of the largest intelligence failures of its history, namely the Yom Kippur War of 1973, when the entire country was caught off-guard by an invasion from Egypt and Syria. Indeed, the Unit only provided several hours' of warning to the rest of the IDF, which did not give the forces enough time to mobilize for immediate defense (Kahana, 2006).

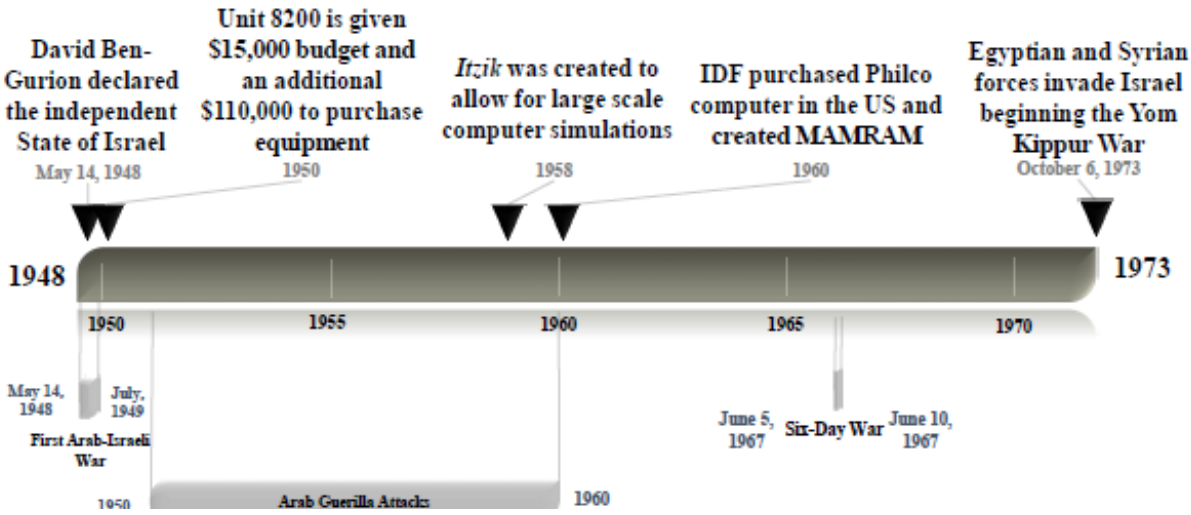



*Figure 1: Unit 8200 History 1948-1973 (Rousseau, 2017)*

Unit 848 had, however, collected vital information in the days preceding the war; not only that the Syrians were bringing bridging tanks up toward the front but also that they were deploying Sukhoi-17 aircraft at unprotected frontline airfields and were moving the Syrian Army's 47th Division from Homs to the Golan Heights (Kahana, 2006). In addition, around twenty hours before the launch of the war, the Unit had also picked up intelligence on an ongoing evacuation process through the Kremlin's awareness of Egypt's and Syria's hostile intentions.

During the war, the Unit is said to have functioned efficiently (Kahana, 2006), helping the IDF to emerge victorious from the eighteen-day war. However, victory came at great human and economic loss, with 2,800 Israelis killed and over 9,000 injured (Shindler, 2008), and economic costs reaching an estimated US$7 billion (Sachar, 1994; in Rousseau, 2017). One particularly important event for the Unit was when one of its intelligence officers was taken captive by the Syrians and subsequently provided his captors with significant information (Behar, 2016).

In the wake of the war, a special investigation led by the Agranat Commission was launched to examine the reasons for this intelligence failure. Its results were two-pronged: Firstly, there had been a general sense of overconfidence among the intelligence community and the IDF in general, which was instilled by the success of the Six-Day War. According to the commission's interim report, this translated into a generalized misconception and complacency – shared notably by the commander of the Unit – that:

*"Egypt would not launch war against Israel before she had first ensured sufficient air power to attack Israel in depth, and in particular Israel's principal airfields, so as to paralyze the Israeli air force, and b) that Syria would only launch an all-out attack on Israel simultaneously with Egypt"* (Agranat Commission of Inquiry, 1974)

Accordingly, while the Unit had "previously deployed special collection means in Egypt, the director of military intelligence at the time, Major General Eliyahu (Eli) Zeira, decided not to activate them, which resulted in concrete early warning evidence of last minute Egyptian preparations for war to be missed" (Kahana, 2006). This ties in with the second problem identified at the time, namely that several officers had dismissed signs and evidence presented by lower-ranking soldiers which could have been used to initiate a much quicker response (Rousseau, 2017).

The inquiry, which ended with the publication of the report in 1975, led to a great deal of national and internal introspection. This in turn resulted in a complete overhaul of the intelligence system to align it with Israel's very unique intelligence needs, given the country's regional context. This change started with the resignation of several senior intelligence officers, notably the Chief of Military Intelligence, Major General Eliyahu Zeira. In addition, the Prime Minister of Israel, Golda Meir, also resigned in the light of public outcry.

A new unit called *Ipkha Mistabra*, or "Devil's Advocate was subsequently established under Military Intelligence" to foster an alternative explanation to mainstream intelligent reports from the establishment (Kahana, 2006).

Meanwhile, Unit 848 not only changed its name to another random number, namely 8200, but was also completely restructured, becoming entirely departmentalized in the process (Behar, 2016). As a result, the Unit's various teams have functioned more or less independently since and remained in the dark about each other's activities.

Furthermore, Israel's military leadership decided to pursue a complete overhaul of the army's early warning system – with Unit 8200 at its center. Following this decision, the Unit received not only more funding, but was also given the privilege to pick the best recruits. In addition, it would no longer focus on a small number of large, expensive projects, but was instead ordered to break up into small, flexible teams tasked with finding quick technical solutions to the concrete needs of the intelligence services (Buck, 2011).

The Yom Kippur War also had lasting effects on the culture of the Unit (and the rest of the IDF). Indeed, while questioning authority had been tolerated within the Unit to a certain extent before the war, it came to be expected and encouraged after (again to a certain extent). Furthermore, the sense of invincibility inherited from the Six-Day War was very much diminished.

Another, more general consequence of the war was that Israel felt it could no longer risk being solely reliant on others – i.e. the US tech industry – to provide it with new technologies. As a result, the IDF invested strongly in Unit 8200 in terms of both personnel and funding to turn it into the country's internal R&D lab (Behar, 2016). This step was taken in parallel to a sharp shift in the source of the IDF's military procurement, which switched from mostly European to mostly US suppliers (Shamir, 2005). The resulting expansion of military equipment transfers, military aid and technological ties drastically boosted numerous local computer science technology companies, many of which developed strong ties with the military (Shamir, 2005).

# 3 Operational Background

This chapter aims at addressing several simple questions relating to the Unit's operational background: What does the Unit do in general? What is it able to do? What operations is it known for? And what operations is it suspected of having conducted? The aim here is not to provide a complete list of the Unit's activities, which is impossible given the limited literature that is publicly accessible, but instead to give an overview of its most salient aspects.

## 3.1 Unit mandate, activities and capabilities

According to one Reserve colonel, the Unit's central mission is to "save lives, prevent terror and other attacks" (Ourcrowd, 2014)[3]. While the Unit's mandate is apparently defensive per nature, this does not stop it from using offensive means to achieve its ambitious objectives pre-emptively. As part of its mandate, the Unit serves as Israel's main signal intelligence (SIGINT) collection service with a specialization in electronic warfare and code decryption. As expressed by a senior Unit 8200 officer, "a part of 8200 deals with operational activity beyond the borders (i.e. EMEA region and Palestinian territories). Our missions include incorporating offensive cyber tools as well as tools that help shape perception, alongside cyber defense" (Zitun, 2016). Its mandate is thus similar to the American NSA or Britain's GCHQ.

More specifically, the Unit's SIGINT activities cover a wide range of tasks from the analysis of information in the public domain to the use of human operators and special signal intelligence (Reed, 2015). Unsurprisingly, they also comprise the interception of various types of communications (i.e. spying), their translation, decryption and analysis. Furthermore, the Unit also engages in offensive and defensive cyber operations (cf. the next sub-chapter). Overall, the Unit attaches importance to operational flexibility, which is supported by rather generous legislative restrictions.

Regarding the points raised above, *Le Monde Diplomatique* claimed in 2010 (Hager, 2010) that the Unit was operating a massive international spying and listening network through its various SIGINT bases. Indeed, thanks to its large antennas and receptors, its Urim base (cf. 4.1) is apparently able to monitor the phone calls, emails, and other communications of both friendly and enemy nations across the Middle East, Europe, Asia, and Africa. According to the same article, the Urim base also has the infrastructure to tap underseas cables (e.g. Mediterranean cables linking Israel to Europe via Sicily) and track global ship traffic (Hager, 2010). In addition, the Unit also reportedly maintains covert listening posts in Israeli embassies abroad as well some covert listening units in the Palestinian territories. Furthermore, it also uses Gulfstream jets equipped with electronic surveillance capabilities to gather data (Hager, 2010).

Most of this data is shared internally across the IDF (as well as sometimes externally, cf. 3.3 below) to the Unit's relevant stakeholders, whether combat troops, decision-makers or other intelligence agencies such as Mossad. Or as Yair Cohen, who served 33 years in Unit 8200, the last five (2001–05) as its commander, put it, "90% of the intelligence material in Israel is coming from 8200 […] there isn't a major operation, from the Mossad or any intelligence security agency, that 8200 is not involved in" (Behar, 2016). It is also suspected that the Unit is somewhat involved with more gruesome elements of the IDF by helping them track and providing intelligence on specific (assassination) targets (Silverstein, 2017). A commonly cited, albeit unverified example from the literature is the assassination in Dubai of Mahmoud al Mabouh, a founder of a Hamas brigade, which mostly implicated Mossad.

Very little is known about the modus operandi and real capabilities of the Unit. However, according to Reed (2015), the Unit has been expanding its focus more on more to include data mining techniques in addition to the gathering of raw data. This includes specifically the ability to look into a great volume of data and metadata and identify menacing messaging or recurring patterns that need to be reflagged (Reed, 2015). Similar to other spy agencies, the Unit is also developing hacking and predictive tools and technologies as well as artificial intelligence (Reed, 2015).

## 3.2 Attributed and alleged operations

Referencing and discussing attributed and alleged activities of Unit 8200 is a complex task for various reasons – firstly, and unsurprisingly, the inherent aura of secrecy surrounding these activities. The second reason, however, is linked to geopolitical considerations and allegiance in cyberspace. More specifically, due to the background of most cybersecurity researchers and companies, there is a clear bias when it comes to attribution and public reporting regarding Western countries such as Israel. This is also linked to the fact that many of these companies' researchers are in fact alumni of the Unit. Therefore, in order to highlight some of its recent activities, the following paragraphs are based on both a

[3] As a caveat, it is venture capitalists that crowdsource Israeli high-tech companies, and many of them are start-ups founded by Unit 8200 alumni.

*cui bono* logic and existing reports, accusations and attestations in relation to cyber-incidents.

The following list identifies the major cyber-related incidents attributed at least in part to Unit 8200 (Cyber Fusion Team, 2018):

- **Stuxnet Virus** (2005–2010): The virus successfully disabled the nuclear centrifuges in Natanz. According to some accounts, the virus was part of the joint Operation Olympic Games between the United States' NSA and Israel's Unit 8200 (Sanger, 2012; Symantec, 2011).
- **Operation Orchard** (September 2007), in which Unit 8200 most probably jammed Syrian radar systems without alerting air defense operators in order to allow for a precise airstrike against a Syrian nuclear facility in Deir ez-Zor (Gross, 2018; Raviv and Melman, 2018). Unit 8200 conducted SIGINT to locate the facility and caused the anti-aircraft defense to malfunction during the attack, leveraging electronic sabotage.
- **Operation Full Disclosure** (March 2014), in which an Israeli commando intercepted an Iranian ship in the Red Sea, which carried military arms and equipment destined for Hamas. The operation was made possible by the Unit's intelligence obtained through "advanced cyber and communications capabilities" (BBC News, 2014; Dombe, 2014).
- **The Ogero Incident** (May 2017), in which the Lebanese government blamed Israel of having launched a sophisticated cyberattack on the state's telecommunications company Ogero to spread disinformation through audio messages to over 10,000 Lebanese citizens, namely that Hezbollah's leader was behind the death of the group's top military commander (The Associated Press, 2017).
- **ISIS terrorist plot thwarted** (February 2018): Unit 8200 discovered and prevented a potential terrorist attack by ISIS against a civilian airliner headed from Australia to the United Arab Emirates. It notably shared its intercepted communications with the Australian authorities to prevent the attack (IDF, 2018).

In addition to these activities, the Unit should be credited for having helped to prevent other sophisticated plots. These include several Iranian cyberattacks against private and public organizations in Israel, Turkey, Qatar, Kuwait, the United Arab Emirates, Saudi Arabia and Lebanon as well as various attacks against Israel by lone-wolf Palestinians in the West Bank (Zitun, 2018). Other alleged unattributed but suspected campaigns and malware linked to Israel and Unit 8200 include the following (Cyber Fusion Team, 2018):

- **Flame** (2007–2012), a sophisticated multi-functional modular malware apparently produced by a sophisticated team for the purposes of cyberespionage. The targets spanned across Iran, Israel and the Palestinian territories. According to an ArsTechnica article (Goodin, 2012), the malware also allegedly infected some Iranian oil facilities. It reportedly also shared similarities (i.e. a common plugin) with an earlier version of Stuxnet. Meanwhile, an article by the Washington Post suggested that the purpose of the Flame cyberespionage campaign was to provide intelligence for the Stuxnet cyberattack (Bencsath et al., 2012; Nakashima and Miller, 2012).
- **Duqu** (2009–2011) was another complex, multi-stage malware that targeted industrial systems manufacturers in over twelve countries, including Iran and Sudan but also Hungary. According to Kaspersky, the malware shared a common development platform, the "Tilded" framework, with Stuxnet (Bencsath et al., 2012; Gostev and Soumenkov, 2011).
- **Gauss** (2011–2012) was a cyberespionage toolkit made for stealing system information and sensitive data. It affected thousands of victims, most of them located in Lebanon, Israel and Palestine. The malware exploited the same vulnerability as Stuxnet and Flame (Bencsath et al., 2012) .
- **miniFlame** (2012) was a sophisticated cyberespionage malware targeting fewer than one hundred machines in Lebanon, Iran, Kuwait, Qatar and the Palestinian Territories. Its backdoor was identified to be one of four malware clients that communicated on the same C2 protocol as Flame. According to Kaspersky, it operated as a previously unknown module in Flame and Gauss (GReAT, 2012).
- And finally, **Duqu 2.0** (2014–2015), a variant of Duqu, was a sophisticated cyberespionage malware operation that targeted organizations and venues linked to the P5+1 Iran Nuclear Agreement negotiations in Vienna and Switzerland (Kaspersky Lab, 2015). According to an article by The Guardian, the sophistication and context of the malware strongly ties it to Israel (Gibbs, 2015).

## 3.3 International efforts and cooperation

The Israeli intelligence community is widely known to cooperate with its partners, which often include Britain, Canada and the US (Sledge, 2014).

According to various leaks, including the Snowden leaks, Unit 8200 has developed a close partnership with the latter and its NSA (Greenwald, 2014; Sledge, 2014). Indeed, according to leaked documents, the NSA "maintains a far-reaching technical and analytic relationship with the Israeli SIGINT National Unit (ISNU) [aka. Unit 8200] sharing information on access, intercept, targeting, language, analysis and reporting." (Greenwald et al., 2013). Furthermore, and among others, both agencies signed a memorandum of understanding in 2009, in which they agreed that the NSA would provide the Unit with raw American SIGINT (Bamford, 2014; NSA, 2009). This included but was not limited to, "unevaluated and unminimized transcripts, gists, facsimiles, telex, voice and Digital Network Intelligence metadata and content." (Greenwald et al., 2013).

The relationship between the two countries' intelligence apparatuses has, however, been a conflicted and challenging one, as has their political relationship. According to Greenwald et al. (2013), stabilizing the SIGINT exchange has been a constant struggle. Overall, "in the last decade, it arguably tilted heavily in favor of Israeli security concerns. 9/11 came, and went, with NSA's only true Third Party [counter-terrorism] relationship being driven almost totally by the needs of the partner." (Greenwald et al., 2013).

Recently, this relationship has been under even greater strain as President Trump was accused of leaking information about ISIS-developed laptop bombs for airplane attacks to the Russian Minister of Foreign Affairs, Sergei Lavrov, during a meeting. Given that this intelligence had been originally provided by the Israelis, the incident quickly turned into a political and diplomatic affair, as Israel considered it a salient breach of the rules of exchange of information (Karmon, 2018).

In addition to the above cooperations, Unit 8200 probably works with many more of its peers, however, there is currently no relevant information in the public domain.

# 4 Organizational and Cultural Background

## 4.1 Organizational structure

It was thus following the Yom Kippur War that Unit 8200 adopted its modern form. While it has changed commanders every four years on average and has been active on many fronts, its general organization and structure have remained quite stable to this day. The following paragraphs detail what is publicly known about this aspect of the Unit.

With regards to the IDF's military structure, Unit 8200 is under the jurisdiction of the IDF Directorate of Military Intelligence or Military intelligence Directorate, aka. Agaf HaModi'in literally meaning "the Intelligence Section" and often abbreviated to AMAN or MID.

AMAN, which is under the aegis of the IDF General Staff, is an independent branch/service of the IDF and the largest component of the Israeli intelligence community (along with Mossad and Shin Bet). Internally, it is made up of three main units, namely Unit 9900 (IMINT), Unit 504 (HUMINT), and, finally, Unit 8200 (SIGINT).

The focus here is Unit 8200 or *Yehida Shmone-Matayim,* which is sometimes also referred to as the Israeli SIGINT National Unit (ISNU). Led by a brigadier-general, it serves as the IDF's main signal intelligence (SIGINT) and decryption unit. Its function is thus comparable to the US American NSA. According to the IDF's own description, "soldiers in the Unit are in charge of the development and use of various information gathering tools and their subsequent analysis, processing and sharing with the concerned stakeholders" (IDF, n.d.).

Interestingly, a 2004 Knesset committee investigating the Israeli intelligence network in the wake of the Iraq war recommended turning the Unit into a civilian national SIGINT agency (as other Western countries have done), but this proposal was apparently not implemented.

In terms of manpower, the Unit is said to represent approximatively 80% of AMAN's manpower. Indeed, according to various sources (Behar, 2016; Nikolic, 2017), its staff ranges between 5,000 and 10,000 members, 5,000 of whom are active at any given time (Behar, 2016). The number of reserves is, however, not available and remains a secret, as is the identity of the current commander, the Unit's budget and the exact number of soldiers and officers. As such, Unit 8200 is one of the largest, if not the largest, units of the IDF.

**Structure and sub-units**

Due to its size, the Unit itself it said to be structured in a rather complex but departmentalized

and flat fashion, a feature that stems from the aftermath of the Yom Kippur War, as shown above. More specifically, the Unit is split up in various small, compartmentalized teams that work individually on task/performance-oriented projects (Senor and Singer, 2009). Teams function in a rather independent, secretive and opaque way, in which adjacent teams often do not know what each other is doing. The teams themselves are not put together according to ranks but rather by disciplines, skills and mix of experience, easily breaking down social and military hierarchies for the sake of project success. Some teams also include so-called "facilitators" experienced in leading and integrating different team members. In addition to its teams, Unit 8200 is also known to comprise several subordinate units.

1. Hatzav

The first of these is **Unit Hatzav**, the open-source intelligence (OSINT) unit within Unit 8200. Accordingly, it is responsible for obtaining military intelligence and counterintelligence from monitoring various world media ranging from television to radio, newspapers, the internet and, more recently, social media (Liphshiz, 2009; Shiviak, 2015). One example of its products are a daily summary and translations of articles from the Arab press, which are published and distributed to intelligence desks and decision-makers (Schleifer, 2005, p. 5). As Hatzav monitors and analyzes media in all major languages, it has actively relied on Arabic, Persian, English, Russian, French and German speakers to translate and research media in those languages (Liphshiz, 2009). According to media reports, the sub-unit provides over half of the overall intelligence information for the Israeli intelligence community (World in War, 2017).

Until 2007, the Unit operated various specialized regional units, such as the *Amichail* unit based in Haifa, whose soldiers were Druze and focused on Lebanese media (Hazkani, 2007). According to reports by *Haaretz* (Cohen, 2016; Ravid, 2012), the then Director of Military Intelligence initially considered closing down the unit before deciding to downgrade it to the point that it is now headed by an officer with the rank of major. Along the way, the unit was split up, and its members were assigned to region-specific (e.g. country or Palestinian Authority) divisions. This reorganization came after several years of neglect, resources constraints and shifting policy priorities. While this step was meant to increase inter-departmental cooperation in monitoring different sources of information, it also came with a number of drawbacks, as some sources (Ravid, 2012) insist that it has affected Israel's intelligence capabilities (Ravid, 2012).

Furthermore, the Unit's media focus changed after the 2011 Arab Spring. Indeed, a decision was then taken to increase military intelligence coverage of Arabic-language social media. According to Israeli government sources quoted by *Haaretz*, this, however, forced a reduction in resources devoted to mainstream media such as television broadcasts. As a result, the IDF has increasingly outsourced some of its intelligence work to two private (right-wing) organizations (i.e. MEMRI and Palestinian Media Watch) for coverage of anti-Israeli material and propaganda in Arab media (Cohen, 2016; Ravid, 2012). Lastly, Hatzav is also pivoting from classic OSINT work toward areas touching on cybersecurity, albeit in an as yet unknown form.

2. Unit 81

The second, even more secretive and more strongly classified sub-unit, **Unit 81**, is AMAN's technology unit. As such, it focuses on researching and supplying state-of-the-art technology (typically integrated hardware-software products) to Israeli combat soldiers (Behar, 2016). According to some estimates, the unit comprises around 1,000 soldiers, or about a fifth of Unit 8200's troops (Behar, 2016).

More generally, instead of relying on outside R&D, the Unit's technologists and researchers often work directly (sometimes on an everyday basis) with intelligence officers to support the various requirements and needs of each project. Accordingly, all of the Unit's technology systems, from analytics to data mining, interception, and intelligence management, are designed and built in-house (Tendler, 2015).

3. Gedasim

The third and last sub-unit is also the most secretive. Sometimes referred to as **Gedasim** or the Sigint Operational Regiment, this unit's function is to collect real-time intelligence on the ground and to transmit it, again in real time, to combat and elite forces (e.g. Shayetet 13 and Sayeret Matkal) to ensure they are able to conduct their missions properly (Zitun, 2016).

**Infrastructure**

Being a SIGINT unit, Unit 8200 operates a great number of bases across the country, many of which are not, for obvious reasons, in the public domain. Nonetheless, some of its principal locations have been disclosed in public or official media. For instance, its headquarters and technical centers have been located at the Glilot Junction north of Tel Aviv since 1954 (Kidon, 2008). It also operates a large base in Herzliya.

The Unit's largest signal intelligence-gathering installation is the Urim SIGINT Base in the Negev desert, approximately 30 km from Beersheba (Hager, 2010). From the exterior, it is described as possessing "lines of satellite dishes of different sizes, barracks and operations buildings on both sides of the road (the 2333) that leads to the base" (Hager, 2010). In addition,

images of the base show 30 listening antennas, making Urim one of the largest signal intelligence bases in the world. According to Hager (2010), the base itself was built several decades ago to monitor satellites (Intelsat) that relay phone calls between countries, but it was subsequently expanded to cover maritime communications (Inmarsat) before targeting other regional satellites.

In addition, the Unit operates smaller bases in various locations, notably in Ora, in Tel Avital (Golan Heights), on Mount Hermon and in Um-Hashiba in the Sinai Desert (Kahana, 2006; Silverstein, 2018, 2016). It also apparently operates – or at least operated – a joint base with the NSA in Ofrit, East Jerusalem (Silverstein, 2014).

Lastly, the Israeli government is currently building a large technology/cyber park called Advanced Technologies Park (ATP) in Beer Sheva. The park, which is intended to become the "cyber center of the western hemisphere" according to Netanyahu, will bring together elements of the private, academic, public and military sectors. Indeed, it combines an office park that will host not only international companies – such as Deutsche Telekom, IBM, Oracle, Lockheed Martin, EMC and PayPal – but also the new governmental National Cyber Bureau and the Cyber Security Research Centre of Beer Sheva's Ben-Gurion University (Reed, 2015). Meanwhile, by the end of 2020, the park will also become home to the new headquarters of the Intelligence Directorate and Communications Division of the Israeli Defense Force (Reed, 2015).

## 4.2 Selection and training process

**Attractiveness and motivation**

Before the release of Senor and Singer's book "Start-up Nation", general awareness, even in Israel, of the Unit and its alumni was close to non-existent. This, however, has changed over the past few years. Nowadays, it is common for its former members and commanders to proudly and publicly showcase – e.g. on their CVs, LinkedIn profiles, etc. – their affiliation to the Unit. As such, this shift has been, in part, an effort by the IDF to market the Unit attractively in order to attract the most talented recruits. Accordingly, it has built up a reputation that draws on two principal aspects to motivate both potential and current recruits: patriotism/duty and financial/career interests.

Regarding the first aspect, the recruits of Unit 8200 are aware, thanks to the increasing publicity of some of its operations (e.g. Stuxnet), of the central role the Unit plays in ensuring Israel's national security. Many of them thus have a strong sense of duty and responsibility towards defending their countrymen, fellow soldiers, friends and family. They feel that their work for the Unit is not only meaningful but also impactful (Reed, 2015). This is particularly reinforced by the fact that they are given great responsibility (i.e. many lives hang on their actions) at a very young age (Bar and Shechter, 2015). This motivation is fueled further by the situational urgency in which Israel and its forces find themselves, notably the proximity and increasing cyber capabilities of Israel's enemies.

In addition to patriotism, a number of the Unit's recruits are also motivated by the success of many of its alumni. Indeed, as it is now commonly known and widely portrayed in the media, the Unit's alumni and commanders have come to found over 1,000 companies and start-ups (e.g. Palo Alto Networks, Checkpoint, Waze, Team8, etc.). There is thus a clear financial incentive to learn the necessary technical skills to create the next big company and possibly make a successful transition to private industry (Rousseau, 2017). This financial incentive also comes into play considering the high cost of higher education in Israel.

In addition, due to the Unit's reputation of being highly competitive, its soldiers are aware that their brothers in arms are some of the country's brightest minds. In a country in which everybody knows everybody and in which common (military) experience is often leveraged for business, there is thus also a strong incentive to maximize time in the Unit to build up a strong and valuable network (Perman, 2005).

**Screening process**

The selection process for Unit 8200 is believed to be one of the IDF's hardest (with the exception of the air force's pilots program) and most clandestine. It is highly competitive, and the Unit competes directly with the other intelligence agencies for the best minds, particularly in the cyber domain.

The selection process for the Unit begins at a young age. Indeed, Unit 8200 starts identifying potential talented recruits as early as in high school. Gifted secondary students are generally screened based on their grades and recommendations from their schools but also from the observations of recruiting officers sent to various schools across the country to identify promising students.

Furthermore, there are two other student pools the Unit pays particular attention to. The first one is the education Ministry's **Gvahim program** (lit. "heights"), which introduced programming and robotics classes to the fourth-grade curriculum in 70 schools (Estrin, 2017). The program mostly targets children in the wealthier central Israel region (Reed, 2015)

The second is the after-school **Magshimim program**, which provides training for gifted high-school computer coders and hackers from underprivileged areas (i.e. southern and northern Israel). The program, which is funded by the Israeli state and the Rashi Foundation, a private organization devoted to helping underprivileged youth, lasts for three years and targets

teenagers aged between 15/16 and 18 years (Estrin, 2017; Reed, 2015). Throughout the program, they meet "two times a week after school for three-hour classes, complete 10 hours of cyber-related homework a week, and participate in workshops twice a year" (Reed, 2015).

The program itself is already very competitive and hard to get into. Indeed, according to Reed (2015), the candidates – over 2,000 per year – need, first, to pass an online/home quiz of riddles and challenges involving math, logic and algorithms. Previous computer expertise is not needed, and they can even look up answers online or ask a parent for help. The idea is to recruit students who are not intimidated by challenges. This initial test is then followed by a battery of more rigorous tests to test their abilities in programming, languages and thinking outside the box. (Reed, 2015).

Interestingly, the program is also used as an avenue for discouraging future black hackers. It is said (Estrin, 2017) that its educators teach a certain degree of "cyber ethics" whilst underlining that those who might be susceptible to criminal activities will not be accepted into the military and will likely ruin their future prospects in the cyber industry.

**Selection process**

The above screening process only produces a certain pre-selection. The real selection process, meanwhile, officially starts when 17-year-old Israeli males and females (with some religious and racial exceptions) are summoned for their draft day. During that day, future recruits are submitted to a battery of aptitude, psychological and medical tests and interviews which are then distilled into a health and psychometric classification (so-called Kaba score) that determines their options for service opportunities (Senor and Singer, 2009).

The Kaba score is made up of three distinct parts for men and two parts for women (IDF, 2016), namely DAPAR, TZADAK, and TZHAR. Together, these tests are used to evaluate Israel's youth and allocate them to the various IDF units (Rousseau, 2017).

The first part (DAPAR) is a psychometric test performed during the initial interview with IDF recruiters. It makes up 50 percent of a male's score and 60 percent of a female's score. These tests are similar to the American SAT and are split up into several sections such as math, reading comprehension, instructions, word analogies, and shape analogies (Rousseau, 2017).

The second part (TZADAK) is an interview which includes a physical and mental assessment. It comprises a verification of census data, a medical examination and a motivation assessment for joining a combat unit. It makes up 33 percent of the Kaba for males but does not count toward the female's score.

The last part of the Kaba (TZHAR) is also known as the Initial Education Score and represents how much formal education a candidate has. It makes up 17 percent of the Kaba for men and 40 percent for women (IDF: Nefesh B'Nefesh, 2015).

Overall, the Kaba is scored on a scale from 41-56. Scores that range from 52-56 allow the recruit to become an officer. Meanwhile, Unit 8200 places special emphasis on the DAPAR score and usually only allows candidates who score in the 89th percentile or above to enter, similar to the cut-off threshold for Ivy League colleges (IDF: Nefesh B'Nefesh, 2015; in Rousseau, 2017)

After this initial draft day, promising aspirants are taken for another half-day of interviews, simulations and tests at a separate location. What is interesting is that the interviews are not conducted by high-ranking or recruiting officers but rather by young Unit 8200 soldiers motivated to find high-quality replacements (Behar, 2016).

This second round of tests differs from the previous one. According to an alumni, the tests serve to measure a wide range of parameters, from recruits' knowledge (e.g. math, language, coding, etc.), curiosity, determination, analytical thinking and leadership skills to their ability to cooperate in teams, adapt rapidly, think out of the box and learn quickly (Choudhury, 2017; Lakin, 2015; Tsipori, 2017).

**Training process**

Once they have been selected and have accepted their affiliation to Unit 8200, new recruits go through specialized military training in which, instead of participating in traditional military drills, they spend most of their time indoors in front of computers and in various classes (Lakin, 2015). The training takes place at the Unit's Glilot Junction base and lasts around six months. The exact methodology and subjects studied are, for obvious reasons, not publicly disclosed, but recent interviews given by alumni allow certain insights into how the Unit trains its newest members.

Unsurprisingly, training is intensive, extending for between 12 to 18 hours per day (Perman, 2005). Indeed, as Arieli notes, "[The new recruit] is put into a small team where they study, brainstorm, train, analyze, and solve problems, from early in the morning to very late at night" (Arieli, 2016; in Behar, 2016). During this "boot camp for the mind", a great variety of subjects is studied, ranging from electronic engineering and coding to Arabic and communication (Behar, 2016). In addition, recruits are taught how to produce and analyze intelligence, leverage SIGINT, and develop data mining techniques. They also participate in regular high-pressure training simulations (Darknet Diaries and Shamban, 2018).

The officers in charge of training are often only a few years older than the new recruits. These officers employ the Planning by Situations (PBS) teaching approach, which was developed by the IDF's MAMRAM computer training center during the 1980's and is similar to the case-study approach used by The Harvard

Business School (Breznitz, 2002; Rousseau, 2017). According to Breznitz, PBS is "a pragmatic holistic approach to the creation and teaching of discrete bodies of processional knowledge." The method focuses on the qualities and skills students need to acquire in order to do their future jobs. These qualities and skills are referred to as "the professional components."

In order to ensure adequate mastery of these *professional components*, instructors develop the course around a "capstone exercise", which is essentially a final project designed to mimic the graduate's required competences and responsibilities (Breznitz, 2002; Rousseau, 2017). In the case of Unit 8200, instructors often combine technical and intelligence problems. A team of new recruits might, for example, have to build a piece of software that decrypts an enemy transmission, then analyze the transmission and suggest a potential course of action (Perman, 2005; in Rousseau, 2017). After this training, soldiers are placed in different sub-units in Unit 8200. While their individual responsibilities might vary, the fundamentals of their work remain the same.

**Service, reserve and alumni**

In Israel, the mandatory military service period varies between 3 years for men and 2 years for women. Members of Unit 8200, however, often see their service extended, sometimes by several years. The average service time, however, is around four years. During that time, recruits commit to working 18 hours a day, seven days a week (Nikolic, 2017).

This system and the average four-year length of service thus allow for a continuous influx of new recruits, with an annual turnover rate of about 25%. This is seen as a great strength by the Unit's commanders, who see new "young, smart, motivated and passionate men and women looking at problems from an entirely new perspective" every year (Behar, 2016). Moreover, this constant churn also forces Unit members to be very disciplined in designing their products, as most of them will not be there once products are put to use.

Once their service is over, most of the Unit's members return to civilian life, pursuing various careers from tech entrepreneurs to politicians. Many of them also pursue university studies. Some are also encouraged by their commanders to pass an accelerated (two times faster) degree in computer sciences during their service (Nikolic, 2017).

Given Israel's reserve-dominated military structure, most Unit 8200 veterans are required to return to the Unit as reserve for up to three weeks a year until they reach their early 40s (Behar, 2016). This allows the younger and older generations to meet, work with each other, exchange thoughts and ideas, and establish ties that can be leveraged later on. Meanwhile, veterans are able to keep up-to-date with the latest technologies developed by their younger successors.

In addition to these yearly refresher trainings, Unit 8200 veterans stay in touch through another channel, namely its alumni network/association, which includes over 15,000 members all over the world. While Israel has a large number of alumni associations for military units, the Unit 8200 association is unique in its focus. Indeed, in contrast to most others, which tend to perpetuate the memory of the fallen, Unit 8200 alumni focus on leveraging the group for business development and networking as well as for talent acquisition and collaboration (Kerbs, 2007).

More specifically, led by prominent alumni in the Israeli entrepreneurial community, the association helps graduates and veterans to find jobs or investment capital, or to recruit new talents for a corporation. This is done through networking events, a dedicated Internet networking site (similar to LinkedIn), and a secret Facebook group for alumni, among others (Kane, 2016). The association also conducts a number of community outreach programs, including a start-up accelerator called 8200 EISP. This accelerator gives relatively new start-ups access to alumni-led workshops, an 8200 alumni network for talent recruitment, personal mentoring by current and former 8200 members, and access to Unit 8200 alumni association events (8200 EISP 2017; in Rousseau, 2017). Interestingly, this accelerator is also open to Arabs and ultra-Orthodox Jews, most of whom do not or cannot serve in the army (Behar, 2016; Reed, 2015).

## 4.3 Internal culture

As any culture, the Israeli (entrepreneurial) culture entails many intricacies and complexities that only Israelis are able to understand fully. This is also true for the culture prevalent in Unit 8200, and it is therefore difficult to grasp this culture completely and accurately. However, based on the examination of various interviews given by some of the Unit's alumni – with all the caveats this comes with in terms of discourse and narrative-building – one can put forward that the Unit embraces and embodies three of Israeli's core values: chutzpah, rosh gadol, davka, and bitzua (Rousseau, 2017).

The first one can be roughly translated as "audacity" (Senor and Singer, 2009)) or "gall, brazen nerve, effrontery, incredible guts" (Rosten, 1968; in Rousseau, 2017). This feature is best observed in the tendency of Unit 8200 soldiers toward disruptive – sometimes rule-breaking – behaviors, and their readiness to challenge the authority of supervisors if they believe they are right about something (Reed, 2015).

The second value means "signaling that the bearer of this head is capable of seeing the big picture, of taking responsibility and initiative, or demonstrating leadership, and going beyond the job description of the

call of duty" (Kordova, 2012). This feature is best seen in the Unit's training, which strongly encourages and builds this sort of analytical thinking, sense of initiative and adaptability. Furthermore, these young soldiers are pushed – often by the circumstances of their missions – to take responsibility for and ownership of their projects, which others' lives may depend on.

The third value can be translated as "gets things done" (Senor and Singer, 2009) or "crusty, resourceful, impatient, sardonic, effective" (Wieseltier, 1985; in Rousseau, 2017). Within the Unit, this translates into a penchant for flexible thinking, innovation and improvisation in order to crack challenges that some may consider impossible – with sometimes very little resources and tight deadlines. Or, as one alumni put it: "Unit members are taught that there's no such thing as impossible, while no is something temporary that can change by persistence and insistence, even if it's the Unit commander himself who said "no" (Kerbs, 2007). This often leads to a certain degree of objective-driven combativeness that has permeated the Unit since its inception.

Accordingly, this is particularly reinforced by the fact that, by design, there is a certain degree of autonomy, as there is "nobody around to tell you how to complete the missions" (Behar, 2016). Indeed, it seems that superiors grant their subordinates a great deal of scope of action by telling them to go figure problems out on their own, as long as they meet their deadlines. Furthermore, according to Buck (2011), the hierarchy is also tolerant of mistakes (to a certain degree, of course), as long as recruits learn from then.

Technical and strategic innovation is thus particularly well-regarded and strongly encouraged throughout the Unit. In order to "preserve the madness" (Orpaz, 2015) and avoid encroaching bureaucracy and complacency, the commanders of the Unit have established a separate department tasked with strategic innovation, and set up various events and internal processes. These include, for instance regular internal hackathons as well as so-called SOOB or "SIGINT out of the box" events.

Similar to Microsoft's out-of-the-box week, the SOOB week has a standardized structure: On the first day, ideas are crystallized. On the second and third days, the product is turned into an archetype. On the fourth day, a presentation is prepared, and on the last day the result is shown to senior intelligence commanders and leaders in the high-tech industry (Orpaz, 2015). Between 2012 and 2015, a total of ten SOOB events were held, with 30 soldiers participating in each and over 80 ideas being "hatched", ten of which have been adopted, and five out of these ten have had a major impact on the Unit (Orpaz, 2015).

Soldiers are also able to submit ideas relating to specific operations or bureaucratic issues internally via a Unit-wide system ominously called Abracadabra. A proposal typically outlines the manpower necessary for the task. Others in the system can then respond by developing the product's technical features and user interface (Orpaz, 2015).

# 5 Discussion and Analysis

Having outlined the historical, organizational, cultural and operational background of Unit 8200, this Technical Analysis now turns to assessing the Unit's strengths and weaknesses in the following paragraphs.

## 5.1 Strengths

According to the literature, strengths are characteristics of the organization that give it an advantage over others. Based on this definition, the following strengths of Unit 8200 can be identified:

- **Human resources:** As shown above, the Unit's staff is estimated to number between 5,000 and 10,000 troops, of which 5,000 are on active duty at any given time (Behar, 2016). While this is inferior to its US American counterpart, the NSA (estimated to be 35,000–55,000[4] in 2013 (Groll, 2013)), it is on par with the British GCHQ (6,132 in 2011/12 (Intelligence and Security and Committee of Parliament, 2013)). Furthermore, when one considers the Unit's size relative to Israel's population (approximately 8 million), its significance is immediately evident. In terms of competitive advantage, such a sizeable force allows the Unit to specialize and develop capabilities in various domains (e.g. data mining, artificial intelligence, etc.), and pursue a wide range of activities and missions (e.g. offensive cyber operations, decryption, etc.). Possible effects of economies of scale may also come into play.

- **Financial resources and infrastructure:** Once again, there is a lack of publicly available data on the exact resources allocated to the Unit. If one, however, considers its size and the sophistication of some of its operations – e.g. Stuxnet, which used four zero-day vulnerabilities – one can assume that it possesses substantial financial resources. Combined with the rich human resources mentioned above, this generous funding allows the Unit to develop and retain a competitive advantage through various channels, including the possibility and ability to conduct numerous operations, sometimes with very limited funds and sometimes at highly sophisticated levels when the need arises. Furthermore, it permits the Unit to conduct its own R&D – notably through Unit 81 – and develop some of the most technologically advanced software and weapons worldwide. Lastly, this level of financial and human resources makes it possible for the Unit to not only maintain and operate an extensive infrastructure (with advanced technologies from antennas to satellites) and large-scale bases (with the Urim base, for example, being one of the world's largest SIGINT bases) but also to invest in new infrastructures.

- **Capabilities and know-how:** in addition to technology, the Unit has, over the past decades, developed considerable intelligence and cyber capabilities. As such, it now possesses an institutional know-how and memory that very few nations can compete with and which is passed on to new recruits during their training year after year (with a 25% churn). This knowledge, which is constantly built on as the Unit completes missions and pursues further innovation, is one of its core strengths in retaining a competitive edge over its enemies and friends alike.

- **Internal culture**: Another key strength of the Unit is its internal culture. Indeed, through clever design – i.e. compartmentalized, small teams with considerable autonomy and a flat hierarchy – the Unit is able to promote a very Israeli entrepreneurial spirit which in turn fosters effective operational innovation despite some levels of scrappiness and improvisation. In addition, the rather egalitarian power structure and camaraderie that follow also significantly help to overcome various biases which exist in civilian society, for example in terms of gender, age or experience. Furthermore, the fact that recruits are given great responsibility at a very young age also helps them mature and gain experience and self-confidence (particularly for women (Asher-Dotan et al., 2018)) before having to face the realities of professional and academic life.

- **Brand and (pre)-screening process:** A core strength identified in this study is the Unit's ability to identify, attract and retain (to some degree) an efficient and highly intelligent workforce. Its continuous access to an abundance of skilled individuals is mainly due to two elements, namely a strong brand image and reputation, and selective (pre)-screening and selection processes. The Unit's brand has been carefully built up and reinforced over the years through alumni initiatives as well as the disclosure of illustrious operations, state

[4] The official numbers are, of course, not disclosed publicly.

discourse/propaganda and interviews with alumni promoting their start-ups. This reputation has in turn created widespread awareness of the Unit and promotes an image that is very attractive to skilled young recruits. Meanwhile, the Unit's screening and selection processes allow it to identify and follow young talents while preparing their development and fostering their capabilities and skills before they even join the Unit. They also ensure that recruiters are able to select candidates that match the Unit's needs.

- **Virtuous circles:** Finally, another great strength of Unit 8200 is the environment to which it has access and in which it operates, notably the close-knit Israeli high-tech community and strong cooperation between the economic, military, governmental and academic sectors (e.g. the Beer Sheva Cyber Park). This environment creates several virtuous circles which benefit both the Unit and the other sectors involved. For instance, the national pool of cyber experts is extensively connected thanks to their time in the Unit or through other channels, such as the Unit's alumni association. This not only fosters trust but also facilitates recruiting processes and minimizes red tape. Meanwhile, Unit alumni serve as points of contact for future cooperation between the Unit and private firms. Furthermore, the Unit (and Israel at large) also benefits (directly and indirectly) from the development of new cybersecurity and cyberdefense technologies and research produced by its partners.

## 5.2 Weaknesses

Weaknesses are characteristics inherent in an organization that disadvantage it in relation to others. Based on this definition, the following weaknesses can be identified in Unit 8200:

- **Political controversies:** Over the past few years, Unit 8200 has become somewhat infamous and highly controversial due to some of its activities. This was notably illustrated in 2014, when 43 reservists denounced – in an open, signed letter – the "unethical" surveillance of Palestinians not involved in violence (Williams, 2014). Such leaks and bad publicity can have harmful repercussions for both the Unit and Israel at large. For instance, some of the Unit's activities and techniques were disclosed while the Unit itself came under stronger scrutiny by both internal and external actors. At the same time, incidents of this nature exacerbate the risk of sowing dissent among the Unit's ranks and set a precedent for future whistleblowers. Also, they can further damage Israel's reputation and increase international pressure.

- **Bureaucratic encroachment:** As mentioned above, the Unit is substantially different from what it used to be in its early days, and it has become one of the largest units within the IDF. As such, and despite its current decentralized architecture, it is prone to a certain level of bureaucratic encroachment, as is the case with any organization of its size. While obviously not a weakness per se, an excessive systematization of internal processes could stifle its exemplary, highly desirable level of innovation. This is an element the Unit is acutely aware of and has already responded to, as seen above, with the "Department of the Law for Preserving Madness" and its various activities (Orpaz, 2015).

- **Exclusionary and elitist recruitment:** According to Johnson et al. (2017) the Unit's recruits come disproportionately from the richer and more highly educated Tel Aviv area (where a number of Unit 8200 alumni work in the tech industry) as well as from elite high-schools (e.g. Leyada, a semi-private Hebrew university high school in Jerusalem). This imbalance could be due to various dynamics, including networking effects and better access to courses that develop the required skillsets needed for the selection process. Again, while not a direct weakness per se, this tendency could lead to instances where the pool of possible recruits is gradually reduced to a narrow set of the population despite dedicated programs (such as Magshimim), and the Unit misses out on other "less fortunate" but gifted recruits as a result. In addition, there is also the risk that the Unit's recruitment may favor a certain elite (e.g. privileged children of alumni). In the medium to long term, this could reinforce existing disparities within the Israeli population (e.g. Israeli Arabs are not allowed to serve) and regions (e.g. Tel-Aviv vs. central Israel) and impact on the country's internal stability.

- **Non-traditional setting**: An additional issue that has been reported on relates to the transition from military to professional activities, as some Unit 8200 alumni have found it difficult to adapt to more traditional professional settings, norms, hierarchies and

structures after having spent a number of years in the Unit. While not a weakness for the Unit itself, this is an issue that can have repercussions on the success of its alumni and the Israeli economy at large.

- **Reputation and increasing capabilities of enemies**: All over the world, Israel's numerous enemies (and allies) are building up their offensive and defensive cyber capabilities. This is bound to lead to some sort of arms race in terms of both sophistication and volume, which will likely increase the cost of the Unit's activities. This aspect is also reinforced by the Unit's reputation, which makes it an increasingly visible and interesting target for future attacks.

- **Political scrutiny and instability:** Given the current political climate in Israel and the various scandals surrounding the Unit (e.g. refuseniks, NSO Group, etc.), increased scrutiny, questioning or regulation of the Unit's activities could disturb its operational processes. The extent of any such disruption would, of course, depend on the situation. For example, a restructuring of the Unit as proposed by the commission installed after the Iraq war in 2004 would drastically undermine some of the Unit's current activities and ties to other military units while destabilizing the tightly balanced Israeli intelligence community.

# 6 Conclusion and Recommendations

In conclusion, and considering the above background and analysis, it is possible to set out a number of general recommendations for any organization or program wishing to learn from Unit 8200. The most important of these are set out below:

- Ensure that adequate **human and financial resources** as well as high-tech infrastructures are allocated to the program.

- Promote the **regular and continuous transmission of know-how** and experience. This includes not only vertical exchanges during the training of recruits but also horizontal sharing between recruits and reservists. This is particularly relevant in the fast-moving tech industry, where government agencies and the tech industry are sometimes desynchronized.

- Foster an **internal culture of entrepreneurship and innovation**. While sometimes difficult in a highly hierarchical structure, this can, for example, be favored through a decentralized project/mission-driven structure (with small, flexible, autonomous teams); a flat hierarchy where function has priority over rank; and regular challenges to members; etc.

- Develop and nurture **ties with the private sector**. This is critical for various reasons, from technological ones to economic ones. As stated above, in this tech domain, networking effects (e.g. through alumni associations or Facebook pages) are important for staying up-to-date and promoting further innovation. Moreover, partnerships and internships give access to first-hand, relevant professional experience for recruits while fostering trust and facilitating recruitment processes.

- Enhance the **general and professional attractivity** of the program for both recruits and future employers. This is particularly important in countries where the opportunity cost of alternative education is relatively low. In practical terms, one could, for example, think of developing well-recognized collaborative or joint certifications or degrees, accelerated university programs for officers or even military scholarships for university studies for some recruits. Furthermore, the unique first-hand experience recruits gain through the program

should be strongly underlined and put forward as a key point.

- Develop **public awareness** of the program and its successes in order to attract the best possible recruits while also sending a strong signal (i.e. regarding deterrence and legitimacy issue). This goes hand in hand with establishing a recognizable brand and strong identity and reputation. This could, for instance, be achieved by increasing the program's public presence, notably at job or student fairs, during hackathons or through visiting after-school programs. Other options would be targeted ads or the use of military apps to promote programs. Furthermore, in light of the reputation the whole cyber domain holds in the public eye, considerable work could also be done around explaining the role and activities of programs in order to dissipate fears.

# 7 Glossary

Attribution problem: Difficulty to determine with certainty the perpetrator of a cyberattack. Attackers are more difficult to identify because of their ability to cover tracks, perform spoof cyberattacks, or falsely flag other actors as perpetrators (Hay Newman, 2016).

Cyber capabilities: devices, computer programs or techniques designed to create degradation, disruption or destruction effects and manipulation of information, information systems and/or networks in or through cyberspace (Brangetto and Veenendaal, 2016).

Hack: Act of entering a system without authorization (Ghernaouti-Hélie, 2013, p. 433).

Malware: Malicious software that can take the form of a virus, a worm or a Trojan horse (Collins and McCombie, 2012, p. 81).

Signal Intelligence: is the intelligence-gathering by interception of signal, whether communications or electronic signals.

# 8 Abbreviations

| | |
|---|---|
| AMAN | Military intelligence Directorate |
| ATP | Advanced Technologies Park |
| GCHQ | Government Communication Headquarters |
| IDF | Israeli Defense Forces |
| ISNU | Israeli Signal intelligence national Unit |
| MAMRAM | Center of Computing and Information Systems |
| NSA | National Security Agency |
| OSINT | Open source intelligence |
| SIGINT | Signal Intelligence |

# 9 Bibliography


Agranat Commission of Inquiry, 1974. Interim Report.

Asher-Dotan, L., Pizov, M., Shamban, S., 2018. Untold story of 8200: A launching point for women in cybersec. RSA Conference 2018, San Francisco.

Bamford, J., 2014. Israel's N.S.A. Scandal [WWW Document]. N. Y. Times. URL https://www.nytimes.com/2014/09/17/opinion/israels-nsa-scandal.html

Bar, M., Shechter, R., 2015. Beyond Israeli Army Unit 8200 – that's not what Startup Nation is all about [WWW Document]. Geektime. URL http://www.geektime.com/2015/05/31/beyond-israeli-army-unit-8200-thats-not-what-startup-nation-is-all-about/

BBC News, 2014. Israel halts "weapons shipment from Iran" [WWW Document]. BBC News. URL https://www.bbc.com/news/world-middle-east-26451421

Behar, R., 2016. Inside Israel's Secret Startup Machine [WWW Document]. Forbes. URL https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine/#232583051a51

Bencsath, B., Pek, G., Buttyan, L., Felegyhazi, M., 2012. The Cousins of Stuxnet: Duqu, Flame, and Gauss. Future Internet 971–1003.

Black, I., Morris, B., 1991. Israel's Secret Wars: A History of Israel's Intelligence Services, Grove Press. ed. New York.

Breznitz, D., 2002. The Military as a Public Space - The Role of the IDF in the Israeli Software Innovation System. MIT Ind. Perform. Cent. 1–46.

Buck, T., 2011. Israel's army of tech start-up [WWW Document]. Financ. Times. URL https://www.ft.com/content/d45b0c5c-1a83-11e1-ae4e-00144feabdc0

Choudhury, S.R., 2017. Former cyber-intelligence sleuths for Israel now work to uncover malicious hackers [WWW Document]. CNBC. URL https://www.cnbc.com/2017/05/11/israel-unit-8200-team8.html

Cohen, G., 2016. Israel Downgrades Its Open-source Military Intelligence Unit [WWW Document]. Haaretz. URL https://www.haaretz.com/israel-news/israel-downgrades-its-open-source-military-intelligence-unit-1.5454845

Cyber Fusion Team, 2018. Spies in the Middle East: Israeli Cyber Operations [WWW Document]. Secur. Alliance. URL https://www.secalliance.com/blog/spies-in-the-middle-east/

Darknet Diaries, Shamban, S., 2018. Darknet Diaries EP 28: UNIT 8200.

Dombe, A.R., 2014. The IDF is Ready for the Cloud Challenge.

Estrin, D., 2017. In Israel, teaching kids cyber skills is a national mission [WWW Document]. APnews. URL https://apnews.com/e477309a4a1e407ca4ae6568d3035625

Florence, R., 2007. Lawrence and Aaronsohn, Penguin Group. ed. New York.

Friedman, M., 1997. The Haganah. Retrieved from Jewish Virtual Library: [WWW Document]. Jew. Virtual Libr. URL http://www.jewishvirtuallibrary.org/the-haganah

Gibbs, S., 2015. Duqu 2.0: computer virus "linked to Israel" found at Iran nuclear talks venue [WWW Document]. The Guardian. URL https://www.theguardian.com/technology/2015/jun/11/duqu-20-computer-virus-with-traces-of-israeli-code-was-used-to-hack-iran-talks

Goldstone, P., 2007. Aaronsohn's Maps: The Untold Story of the Man who Might have Created Peace in the Middle East, Houghton Mifflin Harcourt. ed.

Goodin, D., 2012. Spy malware infecting Iranian networks is engineering marvel to behold [WWW Document]. Ars Tech. URL https://arstechnica.com/information-technology/2012/05/spy-malware-infecting-iranian-networks-is-engineering-marvel-to-behold/

Gostev, A., Soumenkov, I., 2011. Stuxnet/Duqu: The Evolution of Drivers [WWW Document]. Kaspersky Lab. URL https://securelist.com/stuxnetduqu-the-evolution-of-drivers/36462/

GReAT, 2012. miniFlame aka SPE: "Elvis and his friends" [WWW Document]. Kaspersky Lab. URL https://securelist.com/miniflame-aka-spe-elvis-and-his-friends-5/31730/

Greenwald, G., 2014. CASH, WEAPONS AND SURVEILLANCE: THE U.S. IS A KEY PARTY TO EVERY ISRAELI ATTACK [WWW Document]. The Intercept. URL https://theintercept.com/2014/08/04/cash-weapons-surveillance/

Greenwald, G., Poitras, L., MacAskill, E., 2013. NSA shares raw intelligence including Americans' data with Israel [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents

Groll, E., 2013. By the numbers: The NSA's super-secret spy program, PRISM [WWW Document]. Foreign Policy. URL https://foreignpolicy.com/2013/06/07/by-the-

numbers-the-nsas-super-secret-spy-program-prism/

Gross, J.A., 2018. Ending a decade of silence, Israel confirms it blew up Assad's nuclear reactor [WWW Document]. Times Isr. URL https://www.timesofisrael.com/ending-a-decade-of-silence-israel-reveals-it-blew-up-assads-nuclear-reactor/

Hager, N., 2010. Israel's omniscient ears [WWW Document]. Monde Dipl. URL https://mondediplo.com/2010/09/04israelbase

Hazkani, S., 2007. Amichai - IDF's Druze Intelligence Unit [WWW Document]. Reshet 13. URL http://10tv.nana10.co.il/Article/?ArticleID=515298

IDF, 2018. 8200 Unit thwarts an ISIS attack [WWW Document]. IDF. URL https://www.idf.il/en/articles/terror-and-threats/8200-unit-thwarts-an-isis-attack/

IDF, n.d. Military Intelligence Directorate [WWW Document]. Isr. Def. Forces. URL https://www.idf.il/en/minisites/military-intelligence-directorate/

IDF: Nefesh B'Nefesh, 2015. Tzav Rishon (First Notice) and IDF Draft [WWW Document]. Aliyapedia. URL http://www.nbn.org.il/aliyahpedia/army-national-service/idf-sherut-leumi/joining-the-israeli-army-tzav-rishon-first-notice-and-drafting/

Intelligence and Security, Committee of Parliament, 2013. Intelligence and Security Committee of Parliament Annual Report 2012–2013.

Johnson, G., Scholes, K., Whittington, R., Regnér, P., Angwin, D., 2017. Fundamentals of Strategy, Pearson UK. ed.

Kahana, E., 2006. Historical Dictionary of Israeli Intelligence, Scarecrow Press. ed.

Kane, A., 2016. HOW ISRAEL BECAME A HUB FOR SURVEILLANCE TECHNOLOGY [WWW Document]. The Intercept. URL https://theintercept.com/2016/10/17/how-israel-became-a-hub-for-surveillance-technology/

Kaspesky Lab, 2015. The Duqu 2.0 Technical Details.

Kerbs, G., 2007. The Unit [WWW Document]. Forbes. URL https://www.forbes.com/2007/02/07/israel-military-unit-ventures-biz-cx_gk_0208israel.html#633fd3754d3c

Kidon, A., 2008. Unit 8200: In the Beginning [WWW Document]. Isr. Def. Forces. URL https://web.archive.org/web/20090206103120/http://dover.idf.il/IDF/English/News/today/2008n/09/0101.htm

Kordova, S., 2012. Word of the Day Rosh Gadol: What Sort of Head Do You Have? [WWW Document]. Haaretz. URL http://www.haaretz.com/jewish/features/word-of-the-day-rosh-gadol-what-sort-of-head-do-you-have-1.463372

Lakin, R., 2015. The Secretive Israeli Army Unit that Recruits Like Harvard—And Churns Out High-Profile Startups [WWW Document]. Battery. URL https://www.battery.com/powered/secretive-israeli-army-unit-that-recruits-like-harvard/

Liphshiz, C., 2009. Native English Speakers Have Lost Exclusive Status With IDF Intelligence [WWW Document]. Haaretz. URL https://www.haaretz.com/1.5066738

Nakashima, E., Miller, G., 2012. US, Israel developed Flame computer virus to slow Iranian nuclear efforts, official say [WWW Document]. Wash. Post. URL https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html?noredirect=on&utm_term=.17611689cd33

Nikolic, D., 2017. L'unité militaire 8200, la face longtemps cachée de la high-tech israélienne [WWW Document]. Le Temps. URL https://www.letemps.ch/economie/lunite-militaire-8200-face-longtemps-cachee-hightech-israelienne

NSA, 2009. Memorandum of Understanding (MoU) beterrn the National Security Agency/Central Security Service (NSA/CSS) and the Israeli Sigint National Unit (ISNU) Pertaining to the Protection of U.S. Persons.

Orpaz, I., 2015. Of the people who bought you the 8200: Meet the 9900 - the ambitious little sister [WWW Document]. The Marker. URL https://www.themarker.com/technation/1.2603595

Ourcrowd, 2014. Trenches to Traction: How Israel's elite intelligence unit powers the Startup Nation. Ourcrowd.

Perman, S., 2005. Spies Inc. Business Innovation from Israel's Masters of Espionage, Pearson Education. ed.

Ravid, B., 2012. Officials: Israel Outsources Monitoring of Palestinian Media After IDF Lapse [WWW Document]. Haaretz. URL https://www.haaretz.com/1.5178218

Raviv, D., Melman, Y., 2018. Inside Israel's secret raid on Syria's nuclear reactor [WWW Document]. POLITICO. URL https://www.politico.eu/article/israels-syria-inside-secret-raid-on-nuclear-reactor/

Reed, J., 2015. Unit 8200: Israel's cyber spy agency [WWW Document]. Financ. Times. URL https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c

Rosten, L., 1968. The Joys if Yiddish, McGraww-Hill. ed. Tel-Aviv.

Rousseau, J.P., 2017. THE HISTORY AND IMPACT OF UNIT 8200 ON ISRAELI HI-TECH ENTREPRENEURSHIP. Ohio University.

Sachar, H., 1994. History of Israel: Volume II from the Aftermath of the Yom Kippur War, Oxford University Press. ed. New York.

Sanger, D.E., 2012. Obama Order Sped Up Wave of Cyberattacks Against Iran [WWW Document]. N. Y. Times. URL https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Schleifer, R., 2005. Psychological Warfare in the Intifada: Israeli And Palestinian Media Politics And Military Strategies. Sussex Academic Press.

Senor, D., Singer, S., 2009. Start-up Nation: The Story of Israel's Economic Miracle, Hachette Book Group. ed. New York, NY.

Shamir, E., 2005. Computer Science and Technology in Israel, 1950–1980 [WWW Document]. Rutherford J. URL http://www.rutherfordjournal.org/article030111.html

Shindler, C., 2008. History of Modern Israel: Second Edition, Cambride University Press. ed. New York.

Shiviak, R., 2015. An open secret [WWW Document]. Isr. Tody. URL https://www.israelhayom.co.il/article/306035

Silverstein, R., 2018. New IDF Unit 8200 Secret Spy Base Identified in Ora [WWW Document]. Tikun Olam. URL https://www.richardsilverstein.com/2018/06/13/new-unit-8200-spy-base-identified-in-ora/

Silverstein, R., 2017. Unit 8200: 'First We Take Manhattan, Then We Take Berlin,' and Tokyo, and London… [WWW Document]. Tikun Olam. URL https://www.richardsilverstein.com/2017/02/04/unit-8200-first-take-manhattan-take-berlin-tokyo-london/

Silverstein, R., 2016. Israeli Secret Security Sites Revealed [WWW Document]. Tikun Olam. URL https://www.richardsilverstein.com/2016/11/23/israeli-secret-security-sites-revealed/

Silverstein, R., 2014. Secret NSA Satellite Facility Located at IDF Base in Occupied East Jerusalem [WWW Document]. Tikun Olam. URL https://www.richardsilverstein.com/2014/02/10/secret-nsa-satellite-facility-located-in-jerusalem/

Sledge, M., 2014. NSA Has 'Far-Reaching' Partnership With Israeli Intelligence Agency [WWW Document]. Huffington Post. URL https://www.huffpost.com/entry/nsa-partnership-israel_n_5646263?guccounter=1

Tendler, I., 2015. From The Israeli Army Unit 8200 To Silicon Valley [WWW Document]. Tech Crunch. URL https://techcrunch.com/2015/03/20/from-the-8200-to-silicon-valley/

The Associated Press, 2017. Israel Responsible for anti-Hezbollah Propaganda Phone Hack, Lebanon Says [WWW Document]. Haaretz. URL https://www.haaretz.com/israel-news/israel-responsible-for-anti-hezbollah-propaganda-phone-hack-lebanon-says-1.5471465

Tsipori, T., 2017. 8200 graduates aren't like 23 year-olds in Texas or Norway [WWW Document]. Globes. URL https://en.globes.co.il/en/article-8200-graduates-are-not-like-23-year-olds-in-texas-or-norway-1001191294

Williams, D., 2014. Wiretaps against Palestinians are wrong, Israeli ex-spies tell Netanyahu [WWW Document]. Reuters. URL https://news.yahoo.com/wiretaps-against-palestinians-wrong-israeli-ex-spies-tell-073629377.html

World in War, 2017. Unit 8200 #ISRAEL Cyber Warfare Unit [WWW Document]. World War. URL http://www.worldinwar.eu/unit-8200-israel/

Zitun, Y., 2018. IDF's Unit 8200 helped Australia thwart attempt to bomb plane [WWW Document]. Ynet. URL https://www.ynetnews.com/articles/0,7340,L-5124744,00.html

Zitun, Y., 2016. The unit without the name: A rare glimpse into the 8,200 fighters in the field [WWW Document]. ynet. URL https://www.ynet.co.il/articles/0,7340,L-4861591,00.html

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.