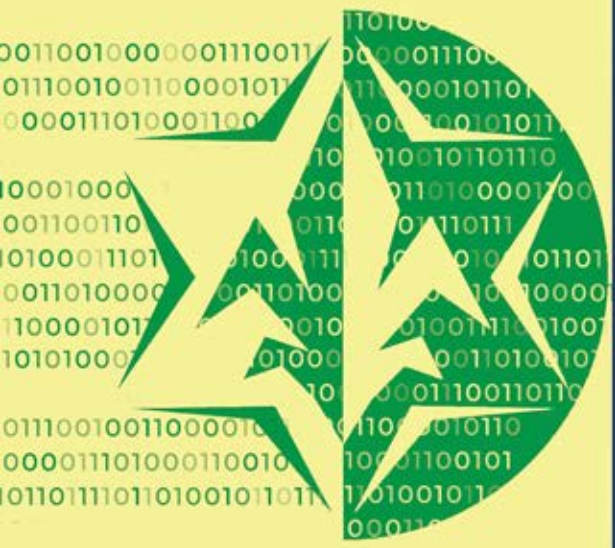
مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

عصر فضای مجازی
صد و سیزدهم



تحلیل روند: یگان ۸۲۰۰ رژیم صهیونیستی
مطالعه‌ای مبتنی بر اوسینت

Trend Analysis : The Israeli Unit 8200, An OSINT-based study

بسم الله الرحمن الرحیم

عصر فضای مجازی

گزارش شماره ۱۱۵

شهریور۱۴۰۱

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

تحلیل روند:
یگان ۸۲۰۰ رژیم صهیونیستی
- مطالعه‌ای مبتنی بر اوسینت

محتوای انتشار یافته در این اثر
الزاماً بیانگر دیدگاه مرکز ملی فضای مجازی نیست

تهیه شده در پژوهشگاه فضای مجازی
(گروه مطالعات فرهنگی و اجتماعی)

مترجم: جلیل ولدخانی
(دانشجوی دکتری جامعه‌شناسی دانشگاه علامه طباطبایی)
علیرضا قبولی شاهرودی
(کارشناسی ارشد جامعه‌شناسی دانشگاه تهران)

ناظر علمی: یحیی شعبانی
(پژوهشگر گروه مطالعات فرهنگی و اجتماعی)
امیررضا باقرپورشیرازی
(مدیرگروه مطالعات فرهنگی و اجتماعی)

نشانی: تهران، میدان آرژانتین، خیابان بیهقی،
نبش خیابان ۱۶ غربی، پلاک ۲۰
تلفن: ۸۶۱۵۱۰۶۱-۰۲۱
کد پستی: ۱۵۱۵۶۷۴۳۱۱

فهرست

سخن نخست

سخن نخست

فضای مجازی با شتاب شگرف و رو به تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را درنوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظر می‌رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالاخص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقیت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره‌کننده فضای مجازی و سایه گستری آن در حوزه‌ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن نوینی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته‌اند.

در همین راستا گزارش‌های عصرفضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه فضای مجازی را ارتقاء بخشیده و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سید ابوالحسن فیروزآبادی
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

خلاصه اجرایی

خلاصه اجرایی

هدف

از زمانی‌که دن سنور[1] و سول سینگر[2] نخستین‌بار در کتاب «ملت استارت‌آپ»[3] (۲۰۰۹) سکوت خود را شکستند، مطالب زیادی دربارهٔ یگان اسرائیلیِ مشهور (و بدنامِ) «۸۲۰۰» نوشته شده است و مجموعه مفصلی از ادبیات نظری و مقالات مختلف در پی روشن کردن ابعادِ مختلفِ این یگان رازآلود برآمده‌اند. اما پراکندگی اطلاعات موجود، ارائه یک تحلیل جامع از این یگان را دشوار کرده است. این مسئله بخصوص در خط‌مشی‌گذارانی که خواهان فهم، کپی‌برداری و الهام‌گرفتن از این یگان پُرآوازه هستند، به چشم می‌خورد.

بنابراین، هدف این مطالعه[4] این است این اطلاعات پراکنده را به‌نحوی قابل‌فهم کرده و با یکدیگر ترکیب کند که بتوان به بهترین‌نحو مرز میان اسطوره، پروپاگاندا و واقعیت را شفاف کرد.[5] به بیان دقیق‌تر، این تحلیلِ روند[6] (TA) دو هدف اساسی را دنبال می‌کند. نخست پس‌زمینهٔ تاریخی، عملیاتی، سازمانی و فرهنگی این

1. Dan Senor
2. Saul Singer
3. Start-Up Nation
4. Cordey, S. (2019) Trend Analysis: The Israeli Unit 8200 – An OSINT-based study, Center for Security Studies (CSS), ETH Zürich.
۵. لازم به ذکر است که صحت و سقم مندرجات این مطالعه درباره کشورها، عملیات‌های سایبری و سایر مصادیق، به‌هیچ عنوان، مورد تأیید پژوهشگاه فضای مجازی نبوده و صرفاً به دلیل حفظ امانت علمی ترجمه شده است. م.
6. Trend Analysis

یگان را بررسی می‌کنیم تا فهم ماهیت واقعیِ این یگان و کاری که انجام می‌دهد، برای خط‌مشی‌گذاران آسان‌تر شود. دوم، این تحلیل روند با کاوش در مهم‌ترین نقاط قوت و ضعف یگان، ارزیابی عمیق‌تری از آن به دست می‌دهد. این‌کار خط‌مشی‌گذاران را قادر می‌سازد تا ضمن شناسایی بهترین اقدامات و ارائهٔ پیشنهادهایی برای به‌کاربستن بینش‌های حاصل [از این مطالعه] در شرایط خاص، درک مناسبی نیز از مکانیسم‌های زیربناییِ عملکرد این یگان و [شرایط] موفقیت آن به دست آورند.

نتایج

بر اساس یافته‌های ما، ریشه‌های یگان ۸۲۰۰ را می‌توان تا یگان اطلاعاتی «Shin Mem 2» - که در دورهٔ پیش از استقلال وجود داشت – ردیابی کرد. پس از استقلال، نیروهای مسلح رژیم صهیونیستی[1] (IDF) این یگان را با چند یگان اطلاعاتی و شنود دیگر تلفیق کرده و یک یگان جنگ الکترونیکی به‌نام یگان ۵۱۵ (و بعدها ۸۴۸) را با بودجه‌ای تقریباً ناچیز تأسیس کرد. نقطهٔ عطف این یگان جنگ *یوم کیپور*[2] در سال ۱۹۷۳ بود که باعث آشکارشدن ضعف‌های اطلاعاتی [رژیم صهیونیستی] شد. این جنگ اثری ماندگار و تاریخی داشت و منجر به بازسازی کامل ساختار این یگان (و تغییر نام آن به «یگان ۸۲۰۰») گردید.

این یگان از لحاظ ساختار و سازمان، بزرگ‌ترین یگان در نیروهای مسلح رژیم صهیونیستی است. در این یگان، هزاران سرباز (دست‌کم پنج‌هزار سربازِ فعال) در قالب یگان‌های کوچک‌تر و پایگاه‌های

1. Israel Defense Force

۲. جنگ یوم کیپور (Yom Kippur War) یا جنگ اعراب و رژیم صهیونیستی جنگی بود که از ششم تا بیست‌وپنجم اکتبر ۱۹۷۳ میان سوریه، مصر و با حمایت چند کشور عربی دیگر، با رژیم صهیونیستی اتفاق افتاد.

عملیاتی متعدد و نیز ایستگاه‌های سیّارِ شنود الکترونیک به کار گماشته شده‌اند. یگان ۸۲۰۰ برای ارتقاء سطح کیفی نیروی انسانیِ خود و توانمندی‌های آن، فرآیندی سخت‌گیرانه و رقابتی برای غربال‌گری، انتخاب و آموزش نیروهای جدید – که مجبور به طی کردن دورهٔ خدمت نظامیِ اجباری هستند – طراحی کرده است. [البته این فرآیند] غربال‌گری از دوران دبیرستان و در قالب برنامه‌های دولتی و خصوصی برای جوانان مستعد آغاز می‌شود. در این دوره، آزمون‌های مختلفی از قبیل آزمون روان‌سنجی، مصاحبه‌های تفصیلی و همچنین آزمونی برای سنجش تحصیلات/مهارت در راستای گزینش [نیروها] انجام می‌شود. آموزش‌ها و تعالیمی که در مراحل بعدی ارائه می‌شود، در عین فشردگی، جامعیت نیز دارد و همه چیز را در بر می‌گیرد - از ارتباطات گرفته تا مهندسی برق و مهارت‌های زبان عربی. از نظر ویژگی‌ها[ی نیروها]، تأکید یگان نه‌تنها بر مهارت فنی، بلکه مهم‌تر از آن بر توانایی یادگیری سریع و تفکر انتقادی است. در نتیجه، فرهنگ غالب در یگان، تفکر انعطاف‌پذیر، ابتکار، ریسک‌پذیری، انطباق سریع، کار گروهی و سلسله‌مراتب یکدست.

یگان ۸۲۰۰ دورهٔ فعالیتِ پربار خود را نخست به‌عنوان یگان رمزگشایی و سرویس جاسوسی (شنود) آغاز کرد. این یگان هدایت برخی از عملیات‌های اطلاعاتیِ دفاعی و هجومی در فضای سایبری را بر عهده داشته است؛ که مشهورترین آن‌ها عبارتند از بدافزار استاکس‌نت[1]، عملیات باغ میوه[2] (۲۰۰۷)، عملیات افشای کامل[3] (۲۰۱۴) و واقعهٔ اوگرو[4] (۲۰۱۷). موارد دیگری از قبیل بدافزار فلیم[5]، دوگو[6]، گاوس[7]، مینی‌فلیم[8] و دوگو ۲[9] نیز به این یگان نسبت داده

1. Stuxnet
2. Operation Orchard
3. Operation Full Disclosure
4. Ogero Incident
5. Flame
6. Duqu
7. Gauss
8. miniFlame
9. Duqu 2.0

می‌شود. به‌علاوه، این یگان با آژانس امنیت ملی آمریکا[1] (NSA) نیز همکاری‌های نزدیکی دارد.

فعالیت‌های یگان ۸۲۰۰ علاوه بر نتایج اطلاعاتی و امنیتی، تبعات عمومی‌تری را برای بخش تکنولوژی‌های های‌تک در رژیم صهیونیستی به بار آورده است. بسیاری این یگان را در آینده به‌مثابهٔ مرکز رشدی[2] برای استارت‌آپ‌های موفق [حوزهٔ] امنیت سایبری، سرمایه‌داران خطرپذیر عرصهٔ تکنولوژی و متخصصان امنیت سایبری تصویر می‌کنند. علاوه‌بر وطن‌پرستی، این تصویر نیز یکی از انگیزه‌های مهم جوانان در پیوستن به این یگان است. در مقایسه با مراکز رشد عادی و خصوصی، این یگان با فرهنگ نظامی، مأموریت‌ها، و شبکه روابطِ خاص خود، قادر به پرورش مهارت‌های رهبری، فنی و کارآفرینی در اعضای جوانِ خود بوده و اعتماد زیادی به فارغ‌التحصیلان و دست‌پرورده‌های خود دارد.

بر طبق این گزارش، مهم‌ترین نقاط قوت این یگان عبارتند از منابع انسانی و مالی، دانش‌عملی[3] و مهارت‌های درونی، فرهنگ داخلی، برندسازی، فرآیند گزینش، و همکاری نزدیک با بخش خصوصی. بااین‌حال، مناقشات سیاسی مختلف، دست‌درازی‌های دستگاه بوروکراسی، گرایش‌های نخبه‌گرایانه، مشکلات مربوط به جابجایی اعضا پس از [دوران] خدمت، و افزایش تحقیق‌وتفحص‌های سیاسی، از جمله چالش‌ها و تهدیدهایی است که این یگان با آن‌ها مواجه است. مطالعهٔ حاضر با بررسی این نقاط قوت و چالش‌ها، این پیشنهادات خط‌مشیِ قابل‌تعمیم را برای موفقیت برنامه‌های سایبری ارائه می‌کند:

1. National Security Agency
2. incubator
3. how-know

۱. تأمین مناسب منابع مالی و نیروی انسانی
۲. پیشرفت در انتقال منظم و پیوستهٔ دانش عملی و تجارب
۳. درونی‌کردن فرهنگ کارآفرینی و ابتکار
۴. توسعه و ایجاد پیوندهایی با بخش خصوصی
۵. افزایش جذابیت عمومی و تخصصی برنامه هم برای نیروهای جدید و هم کارمندان آینده
۶. افزایش آگاهی عمومی در مورد این برنامه

مقدمه

مقدمه

امروزه در [حوزهٔ] تکنولوژی‌های های‌تک و امنیت سایبری واژه رژیم صهیونیستی معمولاً تداعی‌کنندهٔ پلتفرم‌های نوآوری، استارت‌آپ‌های موفق، و روابط مستحکم بخش خصوصی با ارتش است. دلایل و مکانیسم‌های این موفقیتِ تکنولوژیک و تجاری سال‌ها به‌طور مفصل مورد مطالعه قرار گرفته است. یکی از کتاب‌های مهم در این حوزه، کتاب ملت استارت‌آپ: داستان معجزهٔ اقتصادی رژیم صهیونیستی است که توسط دن سنور و سول سینگر در سال ۲۰۰۹ منتشر شد. گذشته از تحلیل جذابی که نویسندگان کتاب در مورد موفقیت تکنولوژیک رژیم صهیونیستی ارائه می‌دهند – و ریشهٔ آن را در فرهنگ و تکثر [موجود در] رژیم صهیونیستی و پدیدهٔ خدمت سربازی اجباری و نیز تهدیدی وجودی می‌یابند که اکثر اسرائیلی‌ها آن را حس می‌کنند، اهمیت و جایگاه برجسته این کتاب در این نکته نهفته است که این کتاب نخستین اثری است که سکوت عمومی در مورد یگان نظامی‌ای که تا آن زمان کاملاً ناشناخته باقی مانده بود - یعنی یگان مشهور (و بدنام) ۸۲۰۰– را می‌شکند.

از آن پس مطالب زیادی دربارهٔ این یگان و به‌خصوص دانش‌آموختگان

مشهور و شناخته‌شدهٔ آن نوشته شده است. نوشته‌های مربوط به یگان ۸۲۰۰ را می‌توان به دو دسته تقسیم کرد. نخست، مطالعات آکادمیک‌تری که به‌صورت عام به سیاست‌های دفاع سایبری، ساختار، توانمندی‌ها و عملیات‌های رژیم صهیونیستی می‌پردازد و برخی از مطالعات خاص‌تر دربارهٔ نقش و جایگاه این یگان را نیز شامل می‌شود. دستهٔ دوم یادداشت‌های ژورنالیستی‌ای است که در نشریات تخصصی (در حوزه‌هایی از قبیل [مطالعات] منطقه، اطلاعات، کسب‌وکار، و حوزهٔ نظامی) و یا در مجلات جریان اصلی و در کنار برخی مقالات آکادمیک – مخصوصاً آثار روسو[1] (۲۰۰۷) - به چاپ می‌رسند. معمولاً این مطالب در قالب مصاحبه‌هایی با اعضای سابق این یگان منتشر می‌شود و این افراد در مورد برخی وقایع، روندها و درس‌هایی که در آنجا فرا گرفته‌اند صحبت می‌کنند. سایر مطالب نیز حاوی پژوهش‌هایی دربارهٔ توانمندی‌ها، مأموریت‌ها و پایگاه‌های منتسب به این یگان و نیز رسوایی‌های آن است.

بنابراین، هدف این مطالعه این است که این اطلاعات پراکنده را به‌نحوی قابل‌فهم کرده و با یکدیگر ترکیب کند که بتوان به بهترین نحو مرز میان اسطوره، پروپاگاندا و واقعیت را در مورد یگان ۸۲۰۰ مشخص کرد. این مطالعه دو هدف اساسی را دنبال می‌کند. اولاً به‌دنبال این است که فهم ماهیت واقعیِ این یگان و کارکرد آن برای خط‌مشی‌گذاران آسان‌تر شود. ثانیاً این تحلیل روند خط‌مشی‌گذاران را قادر می‌سازد درک مناسبی از مکانیسم‌های زیربناییِ عملکرد یگان ۸۲۰۰ و [شرایط] موفقیت آن به دست آورده و به مبنایی دقیق برای ارائهٔ پیشنهاد در مورد اقدامات مناسب دست

1. Rousseau

پیدا کنند.

در این راستا، گزارش حاضر به مطالعهٔ ابعاد مختلف یگان ۸۲۰۰ در نیروهای مسلح رژیم صهیونیستی (IDF) می‌پردازد. بخش نخست به بررسی پیشینه و تکامل تاریخی این یگان از زمان استقلال رژیم صهیونیستی اختصاص پیدا کرده است. بخش دوم دربارهٔ سابقهٔ عملیاتی یگان - به‌خصوص حوزهٔ اختیارات، توانمندی‌ها و عملیات‌های ادعاشده - بحث می‌کند. بخش سوم پیش از پرداختن به فرهنگ این یگان، به بافت سازمانی آن - به‌ویژه ساختار، زیرساخت و فرآیندهای گزینش و آموزش – توجه می‌کند. و نهایتاً در بخش پایانی یافته‌های قسمت‌های قبل ترکیب شده و نقاط قوت و ضعف یگان بیان می‌شود. به‌این‌ترتیب، گزارش حاضر با بحث دربارهٔ مجموعه‌ای از پیشنهادهای تعمیم‌پذیر برای سایر سازمان‌های مشابه خاتمه می‌یابد.

سلب مسئولیت

داده‌های این گزارش تماماً برگرفته از منابع اطلاعاتی آزاد[1] و در دسترس همگان (OSINT) است. چنین داده‌هایی علی‌رغم ارزشمند بودن – بخصوص اگر قابلیت ارجاع بین متون را داشته باشند -، ممکن است مسئله‌ساز باشند؛ چرا که هرگز نمی‌توان صحت آن‌ها را کاملاً تضمین کرد. با توجه به سرشت پیچیده این یگان - یعنی مشهور و در عین حال سرّی - بررسی جامع تاریخ، سازمان، عملیات‌ها و قابلیت‌های آن بسیار دشوار است و مطالب بسیاری دربارهٔ خاستگاه و دخالت آن در امور داخلی و خارجی نامعلوم باقی می‌ماند.

1. Open-source

بخش اول

پیشینه تاریخی

بخش اول

پیشینه تاریخی

۱-۱- یگان‌های اطلاعاتی پیش از استقلال

خاستگاه یگان ۸۲۰۰ به فعالیت‌ها و میراث به‌جامانده از برخی از یگان‌های اطلاعاتی و شنود و بازمی‌گردد که اکثرشان در دورهٔ قیمومیت بریتانیا تشکیل شده و در طی قیام ۳۹-۱۹۳۵ اعراب و تا زمان استقلال رژیم صهیونیستی در ۱۹۴۸ بسیار فعال بودند.

در میان این یگان‌های اطلاعاتی مدرن، قدیمی‌ترین یگان نیلی[1] (NILI) - بمعنای «خداوند لایزال رژیم صهیونیستی دروغ نخواهد گفت»[2] نام دارد. این محفل جاسوسی به‌عنوان گروهی سری در خدمت آژانس اطلاعاتی انگلستان بود که اطلاعات مختلفی دربارهٔ عثمانیان (برای مثال تحرکات و آرایش نیروها) و منطقه (برای مثال الگوهای آب‌وهوایی و مسیرهای حمله) به نیروهای مهاجم ارائه می‌کرد (Florence, 2007; Goldstone, 2007; in Rousseau, 2017).

با تجزیهٔ خلافت عثمانی و تأسیس کشور فلسطین تحت قیمومیت بریتانیا (۱۹۴۸-۱۹۲۰)، هگانا[3] یا «دفاع» به‌عنوان گروهی از شبه‌نظامیان مخفی شکل گرفت که وظیفه‌اش محافظت از یهودیان در برابر حملات شبه‌نظامیان عرب بود. در سال ۱۹۲۹، اعضای هگانا یگان

1. Netzah Yisrael Lo Yeshaker (NILI)
2. The Eternal One of Israel will not lie
3. Haganah

Shin Mem را تشکیل دادند که بدل به نخستین یگان شنود الکترونیک (موسوم به SIGINT) شد که اطلاعات رادیویی را تحت‌نظر می‌گرفت و ترافیک سیگنال‌های دشمن را رصد می‌کرد (Black and Morris, 1991; Kidon, 2008). طی سال‌های متمادی و به‌خصوص پس از سرکوب خونین اعراب در شورش ۱۹۲۹ و *قیام بُراق*[1]، هگانا بیش‌ازپیش تبدیل به سازمانی محوری، بالغ و حرفه‌ای شد (Friedman, 1997; in Rousseau, 2017) که در همکاری با سرویس‌های اطلاعاتی بریتانیا، به‌دنبال شبیخون‌زدن به نیروهای اعراب بود (Shindler, 2008; in Rousseau, 2017).

در آن دوران، هگانا چند سرویس اطلاعاتی مخفی تأسیس کرد که مهم‌ترین آن‌ها موساد لا آلیا بث[2] (موساد[3]) و یا «مؤسسهٔ مهاجرت بی»[4] بود که مسئولیت سازماندهی مهاجرت غیرقانونی یهودیان از سراسر قارهٔ اروپا به فلسطین را بر عهده داشت (Schindler, 2008; in Rousseau, 2017). یکی دیگر از این‌گونه سرویس‌های اطلاعاتی *شای*[5] یا «سرویس اطلاعات»[6] نام داشت که به‌عنوان بازوی اطلاعاتی و ضدجاسوسی هگانا عمل می‌کرد و می‌توان آن را نیای اَمان[7] (دایرهٔ ضداطلاعات ارتش رژیم صهیونیستی) درنظر گرفت که بعدها جزو پیشگامان یگان ۸۲۰۰ شدند (Kahana, 2006).

پس از جنگ جهانی دوم سیاست‌های شدیداً ضداسرئیلیِ بریتانیا موجب مبارزه‌ای سازمان‌یافته و علنی علیه قیمومیت بریتانیا [بر این کشور] شد. در اکتبر ۱۹۴۵، هگانا با دو سازمان نیمه‌نظامی دیگر یعنی اتزل[8] و لِحی[9] متحد شد تا جنبش مقاومت یهود متحد[10] یا

1. Buraq Uprising
2. Mossad Le' Aliyah Beth
3. Mossad
4. Institution for Immigration B
5. Sheruth Yedioth (Shai)
6. the Information Service
7. Military Intelligence Directorate
8. Irgun Zevai Le'umi (Etzel)
9. Lohamei Herut Yisrael (Lehi)
10. The Unified Jewish Resistance Movement

جنبش مقاومت متحد[1] را تشکیل دهند. همین گروه‌ها بعدها تزاحال[2] یا نیروهای مسلح رژیم صهیونیستی (IDF) را شکل دادند (Perman, 2005). بعد از این بود که سلسله وقایعی از قبیل حملهٔ ۱۹۴۶ اتزل به ستاد مرکزی بریتانیا در امور فلسطین، تشکیل کمیتهٔ ویژه سازمان ملل دربارهٔ فلسطین، مخالفت با قطعنامه ۱۸۱ مجمع عمومی سازمان ملل متحد، فروپاشی قیمومیت بریتانیا و جنگ داخلی که پس از آن رخ داد، و برخی وقایع دیگر، منجر به آن شد که دیوید بن‌گورین[3] تأسیس دولت مستقل رژیم صهیونیستی را در چهاردهم مِی اعلام کند. بعداً در همان روز، نیروهای نظامی مصر، سوریه، امارت فرااردن[4]، عراق و لبنان به یکدیگر پیوستند و به دولت تازه تأسیس رژیم صهیونیستی در نخستین نبرد از جنگ‌های چندگانهٔ اعراب و رژیم صهیونیستی یورش بردند (Shindler, 2008; in Rousseau, 2017). می‌توان گفت یکی از عوامل پیروزی رژیم صهیونیستی در این جنگ، شبکه‌های اطلاعاتی وسیعی بود که هگانا در طول فعالیت خود در دهه‌های گذشته شکل داده بود (Perman, 2005).

۱-۲- یگان در دورهٔ پسااستقلال: توانمندی‌ها، مأموریت‌ها، اختیارات و تکنیک‌های پیشین

در سال‌های پس از استقلال و نخستین جنگ رژیم صهیونیستی با اعراب، این کشور اقدام به تحکیم ساختارهای دولتی خود و رسمیت‌بخشیدن به آن‌ها کرد. نمونه بارز این ساختارهای رسمی، مثلث سرویس‌های اطلاعاتی رژیم صهیونیستی است: شاباک[5] یا «سرویس امنیت»[6] که آژانس امنیت رژیم صهیونیستی[7] (ISA) نیز

1. United Resistance Movement
2. Tsahal
3. David Ben-Gurion
4. Emirate of Transjordan
5. Shin Bet
6. Security Service
7. Israel Security Agency

نامیده می‌شود؛ موساد[1] یا «مؤسسهٔ اطلاعات و عملیات‌های ویژه»[2]؛ و اَمان[3] یا «دایرهٔ اطلاعات»[4] که به نام دایرهٔ ضداطلاعات ارتش رژیم صهیونیستی[5] نیز شناخته می‌شود.

دایرهٔ ضداطلاعات ارتش رژیم صهیونیستی - یا «اَمان» - یگانِ جنگ الکترونیکِ ۵۱۵ (که در سال ۱۹۶۸به «یگان ۸۴۸» تغییر نام داد) یا «یگان هشدار مرکزی»[6] را در یک عمارت ویلایی مستقر کرد؛ عمارتی در بندر تاریخی یافا[7] که قبلاً متعلق به یک شیخ عرب بود (Kahana, 2006). اسم رمز این گروه «خرگوش» بود و دو بخش اصلی داشت: بخش شنود الکترونیک[8] که می‌کوشید ارتباطات دشمن را رهگیری کند، و بخش رمزگشایی اطلاعات[9] که مسئول رمزگشایی از کدها و کشف معنای داده‌های جمع‌آوری‌شده بود (Kahana, 2006). نکتهٔ جالب توجه این است که بخش اعظمِ توان تکنولوژیکِ این یگان‌ها محصول تلاش اولین مهندسان کامپیوتر رژیم صهیونیستی بود؛ مهندسانی که برخی از آن‌ها از اتحادیهٔ جماهیر شوروی به رژیم صهیونیستی مهاجرت کرده بودند (Shamir, 2005).

این یگان در مقایسه با سایر یگان‌های بزرگ و مدرن نه تنها بسیار کوچک بنظر می‌رسید، بلکه با بودجهٔ بسیار محدودی اداره می‌شده است. بودجهٔ این یگان در سال ۱۹۵۰برابر بود با ۱۵ هزار دلار آمریکا بعلاوهٔ ۱۱۰ هزار دلارِ دیگر که برای تجهیز سخت‌افزارهای الکترونیکی اولیه اختصاص یافته بود - که عمدتاً از منبع مازاد سهام‌های آمریکایی تأمین می‌شد (Perman, 2005). این رقم به

1. HaMossad leModiʿin uleTafkidim Meyuḥadim
2. Institute for Intelligence and Special Operations
3. Agaf HaModi›in lit
4. Intelligence Section
5. Military Intelligence Directorate
6. Central Warning Unit
7. شهر بندری یافا (Jaffa) در کرانه خاوری مدیترانه و در ۶۰ کیلومتری تل‌آویو
8. SIGINT (Signals Intelligence)
9. Deciphering Intelligence

قیمت امروزی حدوداً معادل ۱ میلیون و ۲۵۰ هزار دلار آمریکاست؛ رقمی که چه براساس معیارهای جدید و چه با نظر به معیارهای زمانِ خودش بسیار ناچیز است. در نتیجه، این یگان مجبور بود بخاطر محدودیت بودجه و علاوه‌برآن در جهت پنهان‌نگه‌داشتنِ توان اطلاعاتیِ خود، اکثر سخت‌افزارها و نرم‌افزارهایش را خودش با استفاده از منابع اندک و نیروی انسانیِ محدود توسعه دهد. این روند تا به امروز تداوم داشته است - البته شاید با بودجهٔ اندکی بیشتر (Perman, 2005).

به‌طورکلی، یگان ۵۱۵ در سال‌های اولیهٔ فعالیت خود با محدودیت‌هایی روبه‌رو بود که رقبای غربی با آن‌ها مواجه نبودند؛ بخصوص کمبودهایی که در حوزهٔ تجربهٔ فنی، مؤسسات تکنولوژیک، منابع مالی و نیروی انسانی وجود داشت (Rousseau, 2017). اما اعضای این یگان برای جبران این کمبودها «به تکنیک‌هایی ابتدایی - و البته مؤثر - متوسل می‌شدند تا ارتباطات دشمن را ردیابی و کنترل کنند» (Rousseau, 2017). برای مثال، آن‌ها یک آنتن ساخته‌شده از سیم فلزی را بین دو قطب نصب کردند و آن را به یک هالی‌کرافتر مدل S-۳۸ - که رادیویی محبوب در دههٔ ۱۹۳۰ و ۱۹۴۰ بود - متصل کردند. در مراحل بعدی یگان ۵۱۵ سیستم‌های رصد پیچیده‌تری را تأسیس کرد که اکثراً بر اساس نقشه‌های به‌سرقت‌رفته از بی‌بی‌سی طراحی شده بود (Perman, 2005).

ابتکارعمل و جنگندگی یگان ۵۱۵ محصول ضرورت‌ها و الزاماتی بود که در دورهٔ حملات و تعرض‌های پیوستهٔ چریک‌های عرب در سراسر دههٔ ۵۰ و ۶۰ وجود داشت. براساس همین الزامات و اقتضائات بود

که این یگان - و به‌طورکلی ارتش - پیوسته در تلاش بود تا در همهٔ شرایط برتری و تفوق خود نسبت به دشمن را حفظ کند. بهترین توصیف برای این نوع نگاه واژهٔ عبریِ davka است که معنای تقریبیِ آن در زبان انگلیسی «عداوت و دشمنیِ آگاهانه» است (Rousseau, 2017; Senor and Singer, ۲۰۰۹). پرمن[1] معتقد است یگان ۵۱۵ از همان ابتدای مسیر خود تجسمی از این مفهوم بوده است (Perman, 2005).

یگان ۵۱۵ تا سال ۱۹۵۴ - که از یافا به مقر فعلی خود در تقاطع گلیلوت[2] نقل مکان کرد (Kidon, 2008) - توانسته بود دامنهٔ نفوذ و پایگاه‌های شنود خود را در سراسر رژیم صهیونیستی توسعه دهد.

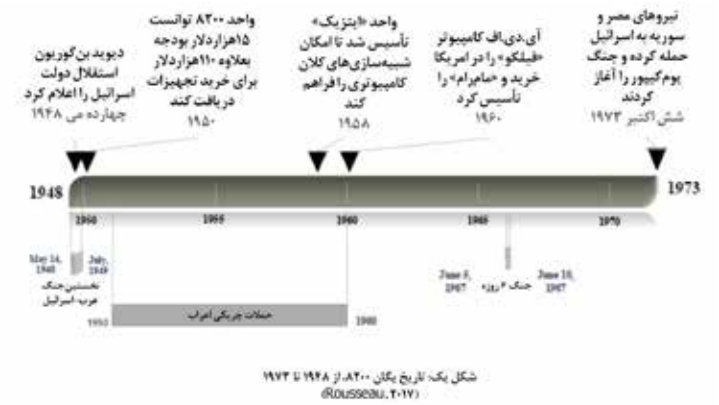
این یگان هیچ‌گاه تلاش خود برای دسترسی به تکنولوژی پیشرفتهٔ کامپیوتری را متوقف نکرد. برای نمونه، واحد تحقیق‌وتوسعهٔ نظامیِ (R&D) در ارتش رژیم صهیونیستی - که رافائل[3] نام داشت و به‌عنوان مسئول ارتقاء تسلیحات نظامی شناخته می‌شد - یکی از نخستین کامپیوترهای آنالوگ رژیم صهیونیستی را در سال ۱۹۵۶ تولید کرد. این واحد در سال ۱۹۵۸ کامپیوتری به نام Itzik تولید کرد که امکان شبیه‌سازی‌های کلان را فراهم می‌کرد. بنظر می‌رسد که این کامپیوتر در اختیار یگان ۵۱۵ قرار گرفته بوده است (Breznitz, 2002; in Rousseau, 2017). دو سال بعد، وزارت دفاع رژیم صهیونیستی یک کامپیوتر فیلکو[4] از ایالات متحده خرید و یک «مرکز کامپیوتر و اسناد مکانیزه»[5] تشکیل داد (Breznitz, 2002; in Rousseau, 2017).

یگان ۵۱۵ و IDF این قدرت محاسباتی جدید را به‌صورت گسترده در جنگ شش روزهٔ سال ۱۹۶۷ به کار گرفته و با کمک آن توانستند ارتباطات نیروی هوایی مصر و سوریه را رهگیری و رمزگشایی کنند.

1. Perman
2. Glilot Junction
3. RAFAEL
4. Philco
5. Merkaz Mahshevim UMa›arahot Meida = The Center for Computers and Mechanized Records

این کار باعث شد که رژیم صهیونیستی با نیروی هوایی کوچک و محدود خود بتواند بر حریم هوایی مسلط شده و آن را به کنترل خود درآورد (Perman, 2005). شکست‌دادن نیروی هوایی مصر، سوریه و اردن در این نبرد کوتاه - که موجب گسترش چشمگیر قلمروی رژیم صهیونیستی شد - حسی از شکست‌ناپذیری را در اسرائیلی‌ها، IDF و بخش اطلاعات بوجود آورد (Senor and Singer, 2009; in Rousseau, 2017).

پس از این جنگ بودجهٔ عظیمی به یگان شنود الکترونیکِ IDF (که اکنون «یگان ۸۴۸» خوانده می‌شود) اختصاص یافت تا توانایی خود در جمع‌آوری اطلاعات - به‌ویژه دربارهٔ سوریه و مصر - را افزایش دهد (Kahana, 2006). چندین مرکز شنود الکترونیک با هدف ثبت و ضبط شواهد و اطلاعاتِ ارتباطی احداث شد - به‌خصوص در تل‌آویتال[1] در بلندی‌های جولان، در جبل الشیخ[2]، و در ام‌هاشیبا[3] واقع در صحرای سینا[4] - تا امکان هشدار به‌موقع در مورد آغاز درگیری فراهم شود (Kahana, 2006).



شکل یک: تاریخ یگان ۸۲۰۰، از ۱۹۴۸ تا ۱۹۷۳ (Rousseau, ۲۰۱۷)

1. Tel Avital
2. Mount Hermon
3. Um-Hashiba
4. Sinai Desert

۱-۳- جنگ یوم کیپور و پیامدهای آن

نقطهٔ عطف یگان ۸۴۸ واقعه‌ای بود که بسیاری آن را بزرگ‌ترین شکست اطلاعاتی تاریخ آن تلقی می‌کنند؛ یعنی جنگ یوم کیپور در سال ۱۹۷۳ که طی آن کل کشور با حملهٔ مصر و سوریه غافلگیر شد. این یگان تا چند ساعت قبل از حمله هشداری به IDF نداده بود. این هشدار زمانی ابلاغ شد که دیگر زمان کافی برای بسیج فوری نیروها وجود نداشت (Kahana, 2006).

بااین‌حال یگان ۸۴۸ چند روز پیش از جنگ توانسته بود به اطلاعاتی حیاتی دست پیدا کرده و متوجه شود که سوری‌ها درحال آوردنِ تانک‌های پُل‌ساز[1] به سوی خط مقدم هستند، و همچنین درحال وارد کردنِ هواپیمای جنگی سوخو-۱۷ [2] در فرودگاه‌های نظامی محافظت‌نشده در خط‌مقدم بوده و لشکر ۴۷ نیروی زمینی سوریه[3] درحال جابه‌جایی از حمص[4] به سمت بلندی‌های جولان است (Kahana, 2006). علاوه‌براین، حدود بیست ساعت پیش از آغاز جنگ، این یگان توانست از طریق اطلاعات کرملین در مورد اهداف خصمانهٔ مصر و سوریه، اطلاعاتی دربارهٔ عملیات تخلیه‌ای به دست آورد که در همان زمان در حال اجرا بود.

گفته می‌شود این یگان برای پیروزی در جنگ هجده روزه کمک مهمی به IDF کرده است (Kahana, 2006). اما این پیروزی هزینه‌های انسانی و اقتصادی زیادی داشت: ۲۸۰۰ اسرائیلی کشته و بالغ بر ۹۰۰۰ نفر زخمی شدند (Shindler, 2008). هزینه‌های اقتصادی آن نیز در حدود ۷ میلیارد دلار آمریکا تخمین زده می‌شود (Sachar, 1994; in Rousseau, 2017). یک رخداد بسیار مهم برای یگان این بود

1. bridging tanks
2. Sukhoi-17
3. Syrian Army's 47th Division
4. Homs

که یکی از افسران اطلاعاتی‌اش توسط سوری‌ها اسیر شد و متعاقباً اطلاعات مهمی در اختیار دستگیرکنندگان خود قرار داد (Behar, 2016).

پس از این جنگ، تحقیقات ویژه‌ای توسط کمیسیون آگرانات[1] برای بررسی دلایل این شکست اطلاعاتی انجام شد. این تحقیقات به ۲ دلیلِ عمده برای این شکست رسید: نخست، حس اعتمادبه‌نفسِ بیش‌ازحد در سازمان‌های اطلاعاتی و به‌طورکلی در IDF - که به‌واسطهٔ موفقیت در جنگ شش روزه در آن‌ها ایجاد شده بود. بنابر گزارش موقت کمیسیون، اعتمادبنفسِ کاذب باعث شکل‌گیریِ این تصورِ غلط - بخصوص در فرماندهٔ یگان - شد که:

«مصر بدون اطمینان‌پیداکردن از قدرت نیروی هواییِ خود برای هجوم همه‌جانبه به رژیم صهیونیستی - به‌خصوص به فرودگاه‌های نظامی اصلیِ این کشور - و در نتیجه زمین‌گیر کردنِ نیروی هوایی آن، حملهٔ خود را آغاز نمی‌کند. ثانیاً سوریه قطعاً هم‌زمان با مصر با تمام قوا به رژیم صهیونیستی حمله خواهد کرد» (Agranat Commission of Inquiry, ۱۹۷۴).

بر این اساس، درحالی‌که یگان «پیش‌تر تجهیزات جمع‌آوری [اطلاعات] ویژه‌ای را در مصر مستقر کرده بود، سرلشگر الیاهو (الی) زعیرا[2] - که در آن زمان سرپرست اطلاعات ارتش بود - تصمیم گرفت این ابزارها را فعال نکند؛ تصمیمی که منجر به غفلت و بی‌خبری از نشانه‌های واضحِ آخرین آماده‌سازی‌های مصر برای جنگ شد» (Kahana, 2006). مشکل دیگری که باعث این وضعیت شد، این بود که بسیاری از افسران نشانه‌ها و شواهدی را که سربازان پایین‌رده ارائه می‌کردند نادیده گرفتند؛ درحالی‌که می‌توانستند با استفاده از

1. Agranat Commission
2. Major General Eliyahu Zeira

این نشانه‌ها، عکس‌العملی بسیار سریع‌تر [در برابر تحرکات دشمنان] طراحی کنند (Rousseau, 2017).

این تحقیقات - که با انتشار گزارش آن در سال ۱۹۷۵ پایان یافت - باعث شد که جریان گسترده‌ای از بازاندیشی و درون‌نگریِ ملی شکل بگیرد. این درون‌نگری منجر به بازسازی کامل سیستم اطلاعاتی رژیم صهیونیستی شد تا با نیازهای اطلاعاتی خاص این کشور - که در بستر شرایطِ منطقه‌ایِ آن شکل گرفته بود - تناسب بیشتری پیدا کند. این تغییرات با استعفای چند افسر ارشد اطلاعاتی - به‌خصوص سرلشگر الیاهو زعیرا، رئیس اطلاعات ارتش - آغاز شد. علاوه‌براین، نخست‌وزیر رژیم صهیونیستی گلدا مئیر[1] نیز به خاطر اعتراضات عمومی شدید استعفا داد.

در پی این اتفاقات، یگان جدیدی به نام Ipkha Mistabra یا «وکیل مدافع شیطان[2] ذیل [سازمان] اطلاعات ارتش تشکیل شد» تا روایت و توضیح دیگری به‌جای گزارش‌های اطلاعاتی رایجی که تا آن زمان توسط [بخش‌های مختلف این] تشکیلات تدوین می‌شد، ارائه دهد (Kahana, 2006).

در این اثنا، یگان ۸۴۸ علاوه بر اینکه نام خود را به یک عدد تصادفی دیگر - یعنی ۸۲۰۰ - تغییر داد، ساختار خود را به‌طور کامل از نو طراحی کرده و برای تمام بخش‌های آن دپارتمان‌های مجزا اختصاص داد (Behar, 2016). در نتیجه، بخش‌های مختلف این یگان از آن زمان کم‌وبیش مستقل عمل کرده و از فعالیت‌های یکدیگر بی‌خبر بوده‌اند.

علاوه‌براین، سران نظامیِ رژیم صهیونیستی تصمیم گرفتند سیستم

1. Golda Meir
2. Devil's Advocate

هشدار مقدماتیِ ارتش را با محوریت یگان ۸۲۰۰، به‌طور کامل بازسازی کنند. با این تصمیم، یگان ۸۲۰۰ نه‌تنها بودجه بیشتری دریافت کرد، بلکه از این امتیاز نیز برخوردار شد که بهترین نیروها را به خدمت بگیرد. همچنین، این یگان دیگر بر تعداد محدودی پروژهٔ بزرگ و گران تمرکز نمی‌کرد، بلکه درعوض قرار بر این شد که به تیم‌های کوچک و منعطفی تقسیم شود که وظیفه‌شان یافتن راه‌حل‌های تکنیکی سریع برای نیازهای ملموس سرویس‌های اطلاعاتی بود (Buck, 2011).

جنگ یوم کیپور همچنین تأثیرات ماندگاری بر فرهنگ این یگان (و کل IDF) داشت. اگرچه پیش از این جنگ نیز تا حدودی امکان پرسشگری از مقامات بالادستی وجود داشت، پس از جنگ چنین کاری تبدیل به یک وظیفه شد و مورد تشویق قرار می‌گرفت (البته بازهم تا حدی معین). به‌علاوه، احساس شکست‌ناپذیری که میراث جنگ شش روزه بود نیز پس از این جنگ تا حدود زیادی از بین رفت.

یک نتیجهٔ عمومی‌ترِ جنگ یوم کیپور این بود که رژیم صهیونیستی پی بُرد که دیگر نمی‌تواند این ریسک را به جان بخرد که برای تأمین تکنولوژی‌های نوین صرفاً بر دیگران - به‌طور خاص بر تکنولوژی ایالات متحده - تکیه کند. بنابراین، آی‌دی‌اف سرمایه‌گذاری عظیمی روی نیروی انسانی و بودجهٔ یگان ۸۲۰۰ کرد تا آن را تبدیل به آزمایشگاه تحقیق و توسعه داخلی رژیم صهیونیستی نماید (Behar, 2016). این اتفاق به موازات چرخش دیگری بود که در منبع تأمین تجهیزات نظامی آی‌دی‌اف رخ داد و از عرضه‌کنندگان اروپایی به‌سوی آمریکایی‌ها تغییر جهت داد (Shamir, 2005). گسترش نقل‌وانتقال

تجهیـزات نظامـی، کمک‌هـای نظامـی و روابـط تکنولوژیـک باعـث تقویـت تعـداد زیـادی از شـرکت‌های محلـی در حـوزه تکنولوژی‌هـای علـوم کامپیوتـری شـد؛ شـرکت‌هایی کـه بسـیاری از آن‌هـا پیوندهایـی قـوی بـا ارتـش برقـرار کردنـد (Shamir, 2005).

بخش دوم

سابقه عملیاتی

بخش دوم

سابقه عملیاتی

هدف این بخش پرداختن به چند پرسش ساده دربارهٔ سابقهٔ عملیاتی یگان ۸۲۰۰ است: به‌طورکلی این یگان چه کاری می‌کند؟ چه کاری می‌تواند انجام دهد؟ به‌خاطر چه اقدامات و عملیات‌هایی مشهور است؟ و مظنون به هدایت کدام عملیات‌ها بوده است؟ هدف ما ارائهٔ فهرست کاملی از فعالیت‌های یگان نیست؛ چرا که اساساً با توجه به محدودیت منابعِ در دسترس، چنین کاری ممکن نیست. در عوض، هدف [ما] مروری بر برجسته‌ترین جنبه‌های آن است.

۲-۱- محدودهٔ اختیارات، فعالیت‌ها و توانمندی‌ها

بنا به نظر یکی از ژنرال‌های ذخیره ارتش، مأموریت اصلی این یگان «حفظ جان آدمیان و جلوگیری از ترور و سایر حملات» است (Ourcrowd, 2014). اگرچه اختیارعمل این یگان بنا به ماهیتِ آن، در حوزه فعالیت‌های تدافعی تعریف شده است، این امر مانع از استفادهٔ این یگان از شیوه‌های تهاجمی برای تحققِ پیش‌دستانهٔ اهداف بلندپروازانه‌اش نشده است. بخشی از دستورکار این یگان این بوده است که با تخصصِ خود در جنگ الکترونیک و رمزگشایی

کدهـا، به‌عنـوان سـرویس اصلـی شـنود الکترونیـک (SIGINT) در رژیـم صهیونیسـتی ایفـای نقـش کنـد. همان‌طورکـه یکـی از افسـران ارشـد یـگان ۸۲۰۰ می‌گویـد: «بخشـی از یـگان ۸۲۰۰ بـا عملیـات برون‌مـرزی سـروکار دارد (یعنـی اروپـا، خاورمیانـه و آفریقـا[1] و قلمروهـای فلسـطینی). مأموریـت مـا شـامل یکپارچه‌سـازی ابزارهـای سـایبری تهاجمـی و نیـز ابزارهـای ادراک‌سـاز، بـه مـوازات دفـاع سـایبری بـود» (Zitun, 2016). بنابرایـن عملکـرد ایـن یـگان مشـابه آژانـس امنیـت ملـی[2] آمریـکا یـا سـتاد ارتباطـات دولتـی[3] بریتانیـا اسـت.

بـه بیـان دقیق‌تـر، شـنود الکترونیـکِ ایـن یـگان، طیـف وسـیعی از اقدامـات مختلـف را در بـر می‌گیـرد؛ از تحلیـل اطلاعـاتِ حـوزۀ عمومـی گرفتـه تـا اسـتفاده از اپراتورهـای انسـانی و بهره‌گیـری از داده‌های سـگینالی خـاص (Reed, 2015). همان‌طورکـه انتظـار مـی‌رود، ایـن فعالیت‌هـا شـامل مـواردی اسـت از قبیـل: رهگیـری انـواع مختلفـی از ارتباطـات (یعنـی جاسوسـی)، ترجمـه، رمزگشـایی و تحلیـل آن‌هـا. به‌عـلاوه، عملیات‌هـای سـایبری تهاجمـی و تدافعـی نیـز در دسـتورکار ایـن یـگان وجـود دارد. روی‌هم‌رفتـه، انعطاف‌پذیـری عملیاتـی بـرای یـگان مهـم اسـت، امـری کـه به‌واسـطۀ سـهل‌گیری سـخاوتمندانه در محدودیت‌هـای قانونـی حمایـت می‌شـود.

بـا نظـر بـه نکات فـوق، روزنامۀ لومنـد دیپلماتیک[4] در سـال ۲۰۱۰ مدعی شـد (Hager, 2010) کـه ایـن یـگان بـا بهره‌گیـری از پایگاه‌هـای شـنود الکترونیـکِ خـود، تبدیـل بـه یـک شـبکۀ جاسوسـی و شـنود بین‌المللـیِ عظیـم شـده اسـت. به‌عنـوان مثال پایـگاه اوریـم[5] (بخـش ۱,۴) - کـه متعلق بـه ایـن یـگان اسـت -، بـا آنتن‌هـا و دریافت‌کننده‌هـای عظیمـی کـه در

1. (EMEA) Europe, the Middle East and Africa
2. National Security Agency (NSA)
3. Government Communications Headquarters (GCHQ)
4. Le Monde Diplomatique
5. Urim

اختیـار دارد، قـادر بـه کنتـرل تماس‌هـای تلفنـی، ایمیل‌هـا و سـایر ارتباطاتِ کشـورهای دوسـت یـا دشـمن در خاورمیانـه، اروپـا، آسـیا و آفریقا اسـت. بنـا بـه ادعـای ایـن گـزارش [در روزنامـه لوموندـ]، پایـگاه اوریـم زیرسـاخت‌هایی بـرای استراق‌سـمع خطـوط کابلـی زیردریایـی (یعنـی کابل‌هـای واقـع در مدیترانـه کـه رژیـم صهیونیسـتی را از طریـق سیسـیل بـه اروپـا متصـل می‌کنـد) در اختیـار دارد و رفت‌وآمـد کشـتی‌ها را ردگیـری می‌کنـد (Hager, 2010). علاوه‌برایـن، گزارش‌هـا حاکـی از ایـن اسـت کـه ایـن یـگان در سـفارت‌های رژیـم صهیونیسـتی در کشـورهای مختلـف و همچنیـن در قلمروهـای فلسـطینی، پایگاهـای مخفیِ شـنود در اختیـار دارد و همچنیـن از جت‌هـای گلف‌اسـتریم[1] مجهـز بـه سیسـتم‌های نظارتـی الکترونیـک بـرای جمـع‌آوری داده‌هـا اسـتفاده می‌کنـد (Hager, 2010).

بیشـتر ایـن داده‌هـا به‌صـورت داخلـی در آی‌دی‌اف بـا افـراد و گروه‌هـای مرتبـط بـه اشـتراک گذاشـته می‌شـود؛ از گروه‌هـای رزمـی و خط‌مشـی‌گذاران گرفتـه تـا سـایر سـرویس‌های اطلاعاتـی مثـل موسـاد (البتـه گاهـی نیـز بیـرون از ایـن سـازمان منتشـر می‌شـود). یِـر کوهـن[2] - کـه ۳۳ سـال در یـگان ۸۲۰۰ خدمـت کـرد و پنـج سـال پایانـیِ دورهٔ خدمتـش را فرمانـدهٔ یـگان بـود) مدعـی اسـت کـه «۹۰ درصـد از محتـوای اطلاعاتـی در رژیـم صهیونیسـتی محصـول کار یـگان ۸۲۰۰ اسـت...، هیـچ عملیـات مهمـی از سـوی موسـاد یـا آژانس‌هـای امنیتـی و اطلاعاتـی دیگـر اجـرا نمی‌شـود کـه یـگان ۸۲۰۰ در آن دخیـل نباشـد» (Behar, 2016). همچنیـن گمـان مـی‌رود کـه یـگان ۸۲۰۰ همکاری‌هایـی بـا عناصـر [و بخش‌هـای] مخوف‌تـر آی‌دی‌اف دارد و ایـن کار را از طریـق کمـک بـه

1. Gulfstream
2. Yair Cohen

آن‌ها در شناسایی و ردیابی سوژه‌های خاص (ترور) انجام می‌دهد (Silverstein, 2017). یک نمونه مشهور از این کار - که البته هیچ‌گاه رسماً تأیید نشده است – قتل محمد المبحوح[1] - از مؤسسین گروه حماس - در دُبی بود که متهم اصلی آن موساد دانسته می‌شد.

در مورد شیوهٔ کار و توانمندی‌های واقعی یگان ۸۲۰۰ اطلاعات زیادی در دست نیست. اما به زعم رید[2] (۲۰۱۵)، این یگان به‌نحوی در حال گسترش دامنه تمرکز خود بوده است تا علاوه‌بر گردآوری داده‌های خام، تکنیک‌های داده‌کاوی را نیز در بر بگیرد. این امر به‌ویژه شامل توانایی یگان در بررسی حجم زیادی از داده‌ها و فراداده‌ها و شناسایی پیام‌های تهدیدآمیز یا الگوهای مکرری است که نیازمند توجه هستند (Reed, 2015). مانند سایر سرویس‌های جاسوسی، یگان ۸۲۰۰ نیز به توسعهٔ ابزارها و تکنولوژی‌های هک و پیش‌بینی و نیز هوش مصنوعیِ خود می‌پردازد (Reed, 2015).

۲-۲- عملیات‌هایی که یگان ۸۲۰۰ مدعیِ اجرای آن‌هاست و یا به آن نسبت داده می‌شود

رجوع به انواع عملیات‌هایی که یگان ۸۲۰۰ مدعی اجرای آن‌هاست و یا دیگران به آن نسبت می‌دهند، به دلایل مختلف کار دشواری بنظر می‌رسد. دلیل نخست - که چندان دور از انتظار نیست - سرشت محرمانهٔ این اقدامات است. بااین‌حال، دلیل دوم [لزوم] وفاداری و رعایت ملاحظات ژئوپولیتیک در فضای سایبری است. به بیان دقیق‌تر، اغلب پژوهشگران و شرکت‌های امنیت سایبری - به‌علت سابقه و پس‌زمینه‌ای که دارند - در توصیف و ارائهٔ گزارشی

1. Mahmoud al Mabouh
2. Reed

عمومی دربارهٔ کشورهای غربی - از جمله رژیم صهیونیستی - آشکارا سوگیرانه عمل می‌کنند. دلیل دیگرِ این سوگیری این است که اکثر این پژوهشگران در واقع دست‌پرورده‌های یگان ۸۲۰۰ هستند. ازاین‌رو، در پاراگراف‌های پیشِ رو براساس منطق ذی‌نفع‌بودن[۱] و همچنین برمبنای گزارش‌ها، اتهامات و شواهد اثبات‌شده دربارهٔ حوادث سایبری، برخی از فعالیت‌های اخیرِ این یگان را تشریح کرده‌ایم.

فهرست زیر سوانح سایبری کلانی که - دست‌کم تاحدی - منتسب به یگان ۸۲۰۰ است، را معرفی می‌کند (Cyber Fusion Team, 2018):

ویروس استاکس‌نت (۲۰۱۰-۲۰۰۵): این ویروس توانست با موفقیت سانتریفیوژهای هسته‌ای در نطنز را از کار بیاندازد. برخی گزارش‌ها حاکی از این هستند که این ویروس بخشی از عملیات مشترک ان‌اس‌ای آمریکا و یگان ۸۲۰۰ رژیم صهیونیستی به نام عملیات بازی‌های المپیک[۲] بوده است (Sanger, 2012; Symantec, 2011).

عملیات باغ میوه (سپتامبر ۲۰۰۷): یگان ۸۲۰۰ به احتمال زیاد سیستم‌های راداری سوریه را بدون هشداری از سوی اپراتورهای پدافند هوایی دچار اختلال کرد تا امکان یک حملهٔ هوایی دقیق علیه تجهیزات هسته‌ای سوریه در دیرالزور[۳] فراهم شود (Gross, 2018; Raviv and Melman, 2018). یگان ۸۲۰۰ از شنود الکترونیک بهره برد تا این تجهیزات را موقعیت‌یابی کند و با نفوذ الکترونیکی موجب اختلال در عملکرد پدافند هوایی سوریه در زمان حمله شود.

عملیات افشای کامل (مارس ۲۰۱۴): در این عملیات گروهی از

۱. منطق ذینفع‌بودن (a cui bono) اشاره به این اصل دارد که برای تعیین مسئول یک فعالیت به این توجه کنیم که چه کسی از آن سود می‌برد.

۲. عملیات بازی‌های المپیک (Operation Olympic Games)، به مجموعه حملات سایبری علیه تأسیسات هسته‌ای ایران گفته می‌شود که به سال ۲۰۰۶ و دوران ریاست‌جمهوری جرج بوش می‌رسد و در دوران ریاست جمهوری اوباما نیز ادامه یافت. در سال ۱۳۹۱ ژنرال بازنشسته جیمز کارترایت این عملیات را افشا کرد. وی خود یکی از طراحان اصلی این حمله بوده است.

3. Deir ez-Zor

کماندوهـای اسـرائیلی یـک کشـتی ایرانـی را کـه حامـل تجهیـزات و سـلاح‌های نظامـی بـرای حمـاس بـود، در دریـای سـرخ توقیـف کـرد. ایـن عملیـات به‌واسـطهٔ اطلاعاتـی طراحـی شـد کـه یـگان ۸۲۰۰ بواسـطهٔ «قابلیت‌هـای ارتباطاتـی و سـایبری پیشـرفتهٔ» خـود بـه دسـت آورده بـود (BBC News, 2014; Dombe, 2014).

واقعـهٔ اوگـرو (مـی ۲۰۱۷): لبنـان رژیـم صهیونیسـتی را متهـم می‌کنـد کـه حملـهٔ سـایبری پیچیـده‌ای را علیـه شـرکت اوگـرو - کـه شـرکت مخابراتـی دولتـی اسـت - طراحـی کـرده اسـت تـا بـا ایـن کار، از طریـق پیام‌هـای صوتـی اقـدام بـه انتشـار اطلاعـات غلـط[1] بـه بیـش از ۱۰ هـزار شـهروند لبنانـی کنـد. ایـن اطلاعـات غلـط در ایـن مـورد بـود کـه رهبـر حـزب‌الله در پشـت پـردهٔ مـرگ فرمانـدهٔ نظامـی عالـی ایـن گـروه بـوده اسـت (The Associated Press, 2017).

جلوگیـری از توطئـهٔ تروریسـتی داعـش (فوریـه ۲۰۱۸): یـگان ۸۲۰۰ حملـهٔ تروریسـتی داعـش بـه یـک هواپیمـای مسـافربری غیرنظامـی از مبدأ اسـترالیا بـه امـارات را کشـف و از آن پیشـگیری کـرد. ایـن یـگان ارتباطـاتِ رهگیری‌شـدهٔ خـود را به‌طـور کامـل در اختیـار مقامـات اسـترالیایی گذاشـت تـا از ایـن حملـه جلوگیـری کننـد (IDF, 2018).

افـزون بـر ایـن اقدامـات، بایـد در نظـر بگیریـم کـه یـگان ۸۲۰۰ بـه پیشـگیری از توطئه‌هـای پیچیـدهٔ دیگـری نیـز کمـک کـرده اسـت؛ از جملـهٔ ایـن توطئه‌هـا می‌تـوان بـه چنـد حملـهٔ سـایبری از جانـب ایـران بـه سـازمان‌های خصوصـی و عمومـی در رژیـم صهیونیسـتی، ترکیـه، قطـر، کویـت، امـارات متحـدهٔ عربـی، عربسـتان سـعودی، لبنـان، و نیـز انـواع حمـلات انفـرادی فلسـطینیان علیـه رژیـم صهیونیسـتی در کرانـهٔ باختـری[2]

1. disinformation
2. West Bank

اشاره کرد (Zitun, 2018). برخی دیگر از عملیات‌ها و بدافزارها نیز هستند که به‌طور قطعی نمی‌توان آن‌ها را به رژیم صهیونیستی نسبت داد، اما ظن و گمانِ این امر وجود دارد. از جملهٔ این عملیات و بدافزارها می‌توان به این موارد اشاره کرد (Cyber Fusion Team, 2018):

فلیم[1] (۲۰۱۲-۲۰۰۷): بدافزار چندمرحله‌ای پیچیده و چندکاره‌ای که ظاهراً توسط یک تیم خبره با هدف جاسوسی سایبری تولید شده و اهداف آن عبارت بوده‌اند از ایران، رژیم صهیونیستی و قلمروهای فلسطینی. بر اساس مقالهٔ آرس‌تکنیکا[2] (Goodin, 2012)، همان‌طور که گفته می‌شود، این بدافزار برخی از تجهیزات نفتی ایران را آلوده کرده است. گفته می‌شود این ویروس شباهت‌هایی با نسخهٔ اولیهٔ استاکس‌نت داشته است (در واقع یک پلاگینِ[3] مشترک داشته‌اند). مقاله‌ای در روزنامه واشنگتن پُست مدعی شده بود که هدف از عملیات جاسوسی سایبری فلِیم، تهیهٔ اطلاعاتی برای حملهٔ سایبری استاکس‌نت بود (Bencsath et al., 2012; Nakashima and Miller, ۲۰۱۲).

دوکو (۲۰۱۱-۲۰۰۹): بدافزار پیچیده و چندمرحله‌ای دیگری است که هدفش سازندگان سیستم‌های صنعتی در بیش از ۱۲ کشور، مثل ایران، سودان و همچنین مجارستان بود. به گفتهٔ شرکت کسپراسکای، پلتفرم توسعهٔ این بدافزار مانند بدافزار استاکس‌نت بوده است – یعنی چهارچوب Tilded[4] (Bencsath et al., 2012; Gostev and Soumenkov, 2011).

گاوس (۲۰۱۱-۲۰۱۲): یک ابزار جاسوسی سایبری که برای استراق داده‌های حساس و اطلاعات سیستم ساخته شده است. این بدافزار غالباً

1. Flame

۲. آرس‌تکنیکا (به انگلیسی: Ars Technica) یا «هنر فناوری» وب‌سایتی است که به اخبار و موضوعات فناوری می‌پردازد. این وب‌سایت به اخباری نظیر سخت‌افزار و نرم‌افزار کامپیوتر، علوم، بازی‌های کامپیوتری و ... می‌پردازد.

۳. اَفزایه (به انگلیسی: Plugin) ابزاری کاربردی و کوچک و وابسته به یک نرم‌افزار میزبان دیگر (مانند مرورگرهای وب) است و به‌تنهایی کاربردی ندارد.

4. Tilded

در لبنـــان، رژیـــم صهیونیســـتی و فلســـطین و ســـایر کشـــورها، هـــزاران قربانـــی داشـــته اســـت. امـــا آســـیب‌پذیری‌ها و نقاط‌ضعـــف گاوس شـــبیه اســـتاکس‌نت و فلیـــم اســـت (Bencsath et al., 2012).

مینی‌فلیـــم (۲۰۱۲): بدافـزار جاسوسـی سـایبری پیچیـده‌ای کـه کم‌تـر از صـد دسـتگاه را در قلمروهـای لبنـان، ایـران، کویـت، قطـر و فلسـطین نشـانه گرفتـه بـود. درِ پُشـتی[1] ایـن بدافـزار به‌عنـوان یکـی از چهـار کارخواه[2] (مشـتری) بدافـزار شـناخته شـده اسـت کـه بـر مبنـای پروتـکل C2 ارتبـاط برقـرار می‌کردنـد. بـه گفتهٔ شـرکت کسپراسـکای، ایـن بدافزار قبـلا به‌صورت ناشـناخته در فلِیـم و گاوس بـه‌کار رفتـه بـود (GReAT, 2012).

دوکـو ۲ (۲۰۱۵-۲۰۱۴): نـوع متفاوتـی از دوکـو در واقـع یـک عملیـات بدافـزار پیچیـدهٔ جاسوسـی سـایبری بـود کـه سـازمان‌ها و اماکـن مرتبـط با مذاکـرات توافـق هسـته‌ای ایـران با گروه پنـج به‌اضافهٔ یک در وین و سـوئیس را نشـانه گرفتـه بـود (Kaspersky Lab, 2015). بر اسـاس مقالـه‌ای از گاردین، پیچیدگـی و بافـت ایـن بدافزار به‌نحوی اسـت که قویـاً می‌تـوان آن را به رژیم صهیونیستی نسـبت داد (Gibbs, 2015).

۲-۳- همکاری‌ها و تلاش‌های بین‌المللی

دسـتگاه اطلاعاتـی رژیـم صهیونیسـتی شـهرت زیـادی در مـورد همکاری بـا شـرکای خـود در عرصـهٔ بین‌المللـی پیـدا کـرده اسـت؛ شـرکایی کـه معمـولاً عبارتنـد از بریتانیـا، کانـادا و ایـالات متحـده (Sledge, 2014). افشـاگری‌های اطلاعاتـی - به‌عنـوان مثـال کار ادوارد اسـنودن[3] - نشـان

۱. درِ پُشتی یا بَک‌دُر (به انگلیسی: Backdoor) در علوم رایانه به راهی گفته می‌شود که بتوان از آن بدون اجازه به قسمت یا قسمت‌های مشخصی از یک سامانه دیگر مانند رایانه، دیوار آتش، یا افزاره‌های دیگر دست پیدا کرد. درهای پُشتی ممکن است از قبل در سامانه وجود داشته باشند یا اینکه فرد نفوذگر با فریب کاربر، او را نسبت به نصب در پُشتی ترغیب کند (مانند ارسال پیوست‌های آلوده در رایانامه).

۲. کارخواه (به انگلیسی client) یا رایانش‌خواه یک نرم‌افزار کاربردی یا سامانه است که از طریق یک شبکه به خدمات یک سامانه رایانه‌ای دیگر به نام سرور یا کارساز دسترسی دارد. این عبارت نخستین‌بار برای افزاره‌هایی که قابلیت اجرای برنامه‌های مستقل خودشان را نداشتند اما می‌توانستند با رایانه‌های دور از طریق شبکه برهم‌کنش داشته باشند، به کار رفت. مدل کارخواه-کارساز امروزه نیز در اینترنت به کار می‌رود. مرورگرهای وب، کارخواه‌هایی هستند که به کارسازهای وب وصل می‌شوند و صفحات وب را برای نمایش بازیابی می‌کنند.

3. Edward Joseph Snowden

داده‌انـد کـه یـگان ۸۲۰۰ همـکاری نزدیکـی بـا ایـالات متحـده و آژانـس امنیـت ملـی (NSA) داشـته اسـت (Greenwald, 2014; Sledge, 2014). برطبـق اسـناد فاش‌شـده، آژانـس امنیـت ملـی امریـکا «رابطـهٔ فنـی و تحلیلـی گسـترده‌ای بـا یـگان ملـی شـنود الکترونیـک رژیـم صهیونیسـتی[1] (ISNU) [ملقـب بـه «یـگان ۸۲۰۰»] داشـته اسـت و ایـن دو اطلاعاتـی در حوزه‌هـای مربـوط بـه دسترسـی، رهگیـری، هدف‌گیـری، زبـان، تحلیـل و گزارش‌دهـی رد و بـدل کرده‌انـد» (Greenwald et al., 2013). به‌عـلاوه، ایـن دو سـازمان در سـال ۲۰۰۹ یادداشـت تفاهمـی امضـا کردنـد کـه براسـاس آن آژانـس امنیـت ملـی امریـکا (NSA) متعهـد شـده اسـت کـه اطلاعـات خـام حاصـل از شـنود الکترونیـک آمریـکا را در اختیـار یـگان ۸۲۰۰ بگـذارد (Bamford, 2014; NSA, 2009). ایـن تفاهم‌نامـه «محتویـات و فراداده‌هـای اطلاعـات شـبکه‌ای دیجیتـال، صـوت، تلکـس، رونوشـت‌ها، نـکات اصلـی و نسـخه‌های ممیزی‌نشـده و کوتاه‌نشـده» را در بـر می‌گیـرد و البتـه محـدود بـه ایـن مـوارد نیسـت (Greenwald et al., 2013).

بااین‌حـال رابطـهٔ بیـن دسـتگاه‌های اطلاعاتـی ایـن دو کشـور، به‌ماننـد رابطـهٔ سیاسـی آن‌هـا پـر تنـش و چالش‌برانگیـز بـوده اسـت. بـه زعـم گرین‌والـد و همـکاران[2] (۲۰۱۳) نزاعـی بی‌پایـان بـرای تثبیـت رونـد مبادلـهٔ اطلاعـات شـنود الکترونیـک در جریـان اسـت. روی‌هم‌رفتـه «در دهـهٔ اخیـر، کفـهٔ ایـن نـزاع بـه نفـع دغدغه‌هـای امنیتـی رژیـم صهیونیسـتی سـنگینی کـرده اسـت. ۱۱ سـپتامبر در حالـی رقـم خورد و سـپری شـد که تنهـا رابطهٔ واقعـیِ آژانـس امنیـت ملـی امریـکا (NSA) بـا یـک طـرف سـوم [در حـوزه ضد-تروریسـم] تقریبـاً به‌طورکامـل براسـاس نیازهـای طـرف مقابـل [یعنـی رژیـم صهیونیسـتی] سـامان پیـدا کـرده اسـت» (Greenwald et al., 2013).

1. Israeli SIGINT National Unit
2. Greenwald et al

اخیراً این رابطه حتی تحت فشار بیشتری نیز قرار گرفته است؛ دونالد ترامپ متهم شد که در جریان جلسه‌ای با وزیر خارجهٔ روسیه، سرگی لاوروف[1]، اطلاعاتی را دربارهٔ بمب‌های لپ‌تاپی ساخت داعش برای حملات هوایی به او منتقل کرده است. از آنجایی‌که این اطلاعات ابتدا توسط اسرائیلی‌ها به‌دست آمده بود، این اتفاق سریعاً بدل به یک مسئلهٔ سیاسی و دیپلماتیک شد؛ زیرا رژیم صهیونیستی آن را نقض آشکار قوانین تبادل اطلاعات می‌دانست (Karmon, 2018).

افزون بر همکاری‌های فوق، یگان ۸۲۰۰ احتمالاً با تعداد بسیار بیشتری از همتایان خود کار می‌کند، اما فعلاً در این‌باره اطلاعات مناسبی به شکل عمومی وجود ندارد.

1. Sergei Lavrov

بخش سوم

پس‌زمینه سازمانی و فرهنگی

بخش سوم

پس‌زمینه سازمانی و فرهنگی

۳-۱- ساختار سازمانی

بعد از جنگ یوم کیپور بود که یگان ۸۲۰۰ به شکلی درآمد که امروز شاهد آن هستیم. علی‌رغم اینکه این یگان در بسیاری از جبهه‌ها فعال بوده و فرماندهان آن به‌طور متوسط هر چهار سال یکبار عوض شده‌اند، ساختار و سازمان کلی آن تا به امروز تقریباً ثابت مانده است. در ادامه جزئیاتی در مورد جنبه ساختاری این یگان - که عمومی شده است - آورده می‌شود.

در ساختار نظامی نیروهای مسلح رژیم صهیونیستی، یگان ۸۲۰۰ از سلسله مراتب قدرت ذیل سازمان ضداطلاعات ارتش (از ارکان آی‌دی‌اف) مشهور به Agaf HaModi›in است که معنای لفظی آن «دایرهٔ اطلاعات» است و اغلب به‌صورت اختصاری اَمان یا ام‌آی‌دی[1] نوشته می‌شود.

اَمان زیر نظر ستاد کل نیروهای مسلح رژیم صهیونیستی و درعین‌حال به‌عنوان یک سرویس عمل می‌کند و بزرگ‌ترین جزء سازندهٔ دستگاه اطلاعاتی رژیم صهیونیستی (در کنار موساد و شین‌بت) محسوب می‌شود. از نظر ساختار درونی، اَمان متشکل از

1. Military Intelligence Directorate (MID)

سه یگان اصلی است؛ یگان ۹۹۰۰ (اطلاعات تصویری)[1]، یگان ۵۰۴ (اطلاعات انسانی)[2] و نهایتاً یگان ۸۲۰۰ (SIGINT).

در اینجا تأکید بر یگان ۸۲۰۰ (به زبان عبری Yehida Shmone-Matay-im) است که بعضاً از آن با عنوان «یگان ملی شنود الکترونیک رژیم صهیونیستی» (ISNU) یاد می‌شود. این یگان که هدایت آن را یک سرتیپ[3] بر عهده دارد، واحد اصلیِ نیروهای مسلح رژیم صهیونیستی در حوزهٔ رمزگشایی و شنود الکترونیک محسوب می‌شود؛ لذا جایگاه آن با آژانس امنیت ملی امریکا (NSA) قابل مقایسه است. بنا بر توصیف نیروهای مسلح رژیم صهیونیستی «سربازان این یگان مسئول توسعه و استفاده از ابزارهای جمع‌آوری اطلاعات مختلف و نیز تحلیل، پردازش و اشتراک‌گذاری آن با افراد [و گروه‌های] مرتبط هستند» (IDF, n.d.).

جالب است که کمیته‌ای از کنست[4] که در سال ۲۰۰۴ مسئول تحقیقات دربارهٔ شبکهٔ اطلاعات رژیم صهیونیستی پس از جنگ عراق بود، توصیه کرد که این یگان به یک آژانس شنود الکترونیک ملی غیرنظامی تبدیل شود (همچنان که سایر کشورهای غربی چنین کرده‌اند)؛ اما از قرار معلوم این پیشنهاد پذیرفته نشده است.

از نظر نیروی انسانی، گفته می‌شود که حدود ۸۰ درصد پرسنل اَمان را نیروهای یگان ۸۲۰۰ تشکیل می‌دهند. براساس منابع مختلف (Behar, 2016; Nikolic, 2017)، کارکنان این یگان بین ۵ الی ۱۰ هزار نفر در نوسان هستند؛ و ۵ هزار نفرشان همواره فعال هستند (Behar, 2016). اما تعداد نیروهای ذخیره غیرقابل‌دسترس و محرمانه است؛ کما اینکه هویت فرماندهٔ فعلی، بودجهٔ یگان، و نیز تعداد دقیق

1. IMINT
2. HUMINT
3. brigadier-general
۴. کِنِست (Knesset) نام پارلمان رژیم صهیونیستی است که در شهر اورشلیم قرار دارد.

سربازان و افسران نیز چنین است. به معنای دقیق کلمه، یگان ۸۲۰۰ اگر بزرگ‌ترین یگان نیروهای مسلح رژیم صهیونیستی نباشد، یکی از بزرگ‌ترین یگان‌های آن است.

ساختار و یگان‌های فرعی

یگان ۸۲۰۰ به علت ابعاد وسیعش، به شیوه‌ای نسبتاً پیچیده ولی سامان‌مند و یکدست سازمان‌دهی شده است؛ خصوصیتی که - همان‌طورکه پیش‌تر نشان دادیم - ریشه در جنگ یوم کیپور دارد. بدنهٔ این یگان به بخش‌های کوچک و مجزایی تقسیم شده است که هر یک بر روی پروژه‌های خروجی‌محور کار می‌کنند (Senor and Singer, 2009). بخش‌های مختلف یگان به شیوه‌ای نسبتاً مستقل، رازآمیز و پیچیده عمل می‌کنند؛ تا حدی که بخش‌های مختلف معمولاً از کار یکدیگر سر در نمی‌آورند. افراد هر بخش و هر تیم نه براساس رتبه، بلکه بر مبنای رشته‌ها، مهارت‌ها و تجارب گرد هم می‌آیند و سلسله‌مراتب نظامی و اجتماعی را به‌راحتی و به‌خاطر موفقیت پروژه‌ها کنار می‌زنند. برخی از این تیم‌ها «تسهیل‌گر»انی نیز در خود دارند که در رهبری و انسجام‌بخشی اعضای مختلف تیم تجربه و تبحر دارند. یگان ۸۲۰۰ علاوه بر تیم‌ها، یگان‌های فرعی مختلفی نیز دارد.

۱. هاتزاو [1]

نخستین نمونه از یگان‌های فرعی، یگان هاتزاو است که زیرمجموعه یگان ۸۲۰۰ بوده و در حیطهٔ منابع اطلاعاتی آزاد (OSINT)

1. Hatzav

فعالیت می‌کند. این یگان مسئول کسب اطلاعات و ضداطلاعات نظامی از طریق رصد رسانه‌های مختلف جهان، شامل تلوزیون، رادیو، روزنامه، اینترنت و اخیراً رسانه‌های اجتماعی است (Liphshiz, 2009; Shiviak, ۲۰۱۵). یک نمونه از خروجی‌های این یگان خلاصه‌های روزانه و ترجمهٔ مقالات از خبرگزاری‌های عربی است که در اختیار میزهای اطلاعاتی و خط‌مشی‌گذاران قرار می‌گیرد (Schleifer, 2005, p. 5). ازآنجاکه هاتزاو رسانه‌های همهٔ زبان‌های اصلی دنیا را رصد و تحلیل می‌کند، مترجمان زبان‌های عربی، فارسی، انگلیسی، روسی، فرانسوی و آلمانی نقش بسیار کلیدی در آن دارند و محتوای این رسانه‌ها را ترجمه و تحلیل و بررسی می‌کنند (Liphshiz, 2009). برخی از گزارش‌های رسانه‌ای مدعی شده‌اند که این یگانِ فرعی تأمین‌کنندهٔ بیش از نیمی از داده‌های اطلاعاتیِ سرویس‌های امنیتی رژیم صهیونیستی است (World in War, 2017).

این یگان تا سال ۲۰۰۷ چندین واحد منطقه‌ایِ تخصصی را مدیریت می‌کرد؛ واحدهایی نظیر AmichaiI در حیفا که سربازان آن دروزی[1] بوده و بر روی رسانه‌های لبنانی تمرکز دارند (Hazkani, 2007). هاآرتص[2] مدعی بوده است که رئیس وقت اَمان ابتدا در نظر داشت که این یگان را تعطیل کند، اما بعداً تصمیم به تنزل رتبهٔ آن گرفت (Cohen, 2016; Ravid, 2012)؛ تا جایی که اکنون توسط یک افسر با درجهٔ سرگردی اداره می‌شود. یگان هاتزاو به‌تدریج دچار انشعاب شد و اعضای آن در بخش‌های ویژه-منطقه‌ای (برای مثال کشور یا تشکیلات خودگردان فلسطین) به کار گرفته شدند. پس از چندین سال غفلت، محدودیت منابع و تغییر در اولویت‌های سیاستی، اکنون

1. Druze
2. Haaretz

شاهد یک باز-سازمان‌دهی در این یگان بودیم که با هدف افزایش همکاری‌های میان‌بخشی در نظارت بر منابع مختلف اطلاعات انجام می‌شد. بااین‌حال، این فرآیند خالی از اِشکال نبود و برخی منابع (Ravid, 2012) مدعی هستند که این اقدام توانایی‌های اطلاعاتی رژیم صهیونیستی را تحت‌الشعاع قرار داده است.

به‌علاوه، تمرکز رسانه‌ای یگان پس از بهار عربی ۲۰۱۱ تغییر کرد و تصمیم بر این شد که پوشش اطلاعات نظامی رسانه‌های اجتماعی عرب‌زبان افزایش پیدا کند. هاآرتص به نقل از منابع دولتی رژیم صهیونیستی مدعی است که این تصمیم موجب کاهش امکانات اختصاص‌یافته به رسانه‌های اصلی - از جمله تلوزیون - شده است. در نتیجه، نیروهای مسلح رژیم صهیونیستی بخشی از وظایف اطلاعاتی خود را به دو سازمان (راست‌گرای) خصوصی (یعنی «مؤسسه پژوهش رسانه‌ای خاورمیانه»[1] و «دیده‌بان رسانه‌های فلسطین») محول کرده است؛ تا مطالب و پروپاگاندای ضد اسرائیلی در رسانه‌های عربی را پوشش خبری دهند (Cohen, 2016; Ravid, 2012). نهایتاً اینکه یگان هاتزاو نیز در حال گذار از کار کلاسیک بر روی منابع اطلاعاتی آزاد به‌سمت عرصه‌های مربوط به امنیت سایبری است؛ البته به شیوه‌ای ناشناخته.

۲. یگان ۸۱

دومین یگان فرعی که از نمونهٔ قبلی بسیار محرمانه‌تر و طبقه‌بندی‌شده‌تر است، «یگان ۸۱» نام دارد که یگان تکنولوژی اَمان به حساب می‌آید. این یگان مشخصاً بر پژوهش دربارهٔ

1. MEMRI

پیشرفته‌ترین تکنولوژی‌ها (نوعاً محصولات سخت‌افزاری-نرم‌افزاری عمومی) و تأمین آن برای سربازان رژیم صهیونیستی متمرکز است (Behar, 2016). بر اساس برخی برآوردها، این یگان از حدود ۱۰۰۰ سرباز تشکیل می‌شود - رقمی که یک‌پنجم جمعیت یگان ۸۲۰۰ است (Behar, 2016).

متخصصان و محققین حوزهٔ تکنولوژی در این یگان به‌جای تکیه بر پروژه‌های برون‌سپاری‌شدهٔ «تحقیق‌وتوسعه» (R&D)، اغلب به‌صورت مستقیم (و بعضاً هر روز) در جهت تأمین نیازها و الزامات پروژه‌های مختلف با مقامات اطلاعاتی تعامل می‌کنند. بنابراین، همهٔ سیستم‌های تکنولوژیک این یگان - از دانش تحلیلی گرفته تا داده‌کاوی، رهگیری و مدیریت اطلاعاتی - در داخل خودش طراحی و ساخته می‌شود (Tendler, 2015).

۳. هنگ عملیاتی شنود الکترونیک[1]: «گِدِسیم»[2]

سومین و آخرین یگان فرعی که محرمانه‌ترینِ آن‌ها نیز هست، گِدِسیم یا هنگ عملیاتی شنود الکترونیک نام دارد. کار این یگان این است که به‌صورت زنده و در لحظه، اطلاعاتِ میدانی را استخراج کرده و به بخش‌های نظامی و سیاسی (مثلاً واحدهای Shayetet 13 و Sayeret Matkal) ارسال کنند؛ تا اطمینان حاصل شود که آن‌ها به‌خوبی قادر به اجرای مأموریت‌شان خواهند بود (Zitun, 2016).

زیرساخت‌ها

یگان ۸۲۰۰ به‌عنوان یک یگان شنود الکترونیک، در سرتاسر رژیم

1. Sigint Operational Regiment
2. Gedasim

صهیونیستی پایگاه‌های بسیاری دارد که - به دلایل واضح - اکثرشان به‌صورت عمومی شناخته‌شده نیستند. بااین‌حال، برخی از اماکن اصلی آن در رسانه‌های عمومی و رسمی افشا شده‌اند. برای نمونه، ستاد اصلی و مراکز فنی آن از سال ۱۹۵۴ در تقاطع گلیلوت در شمال تل‌آویو مستقر شده است (Kidon, 2008). این یگان همچنین پایگاه بزرگی در شهر هرتزلیا[1] در اختیار دارد.

بزرگ‌ترین تأسیسات یگان برای جمع‌آوری اطلاعات شنود الکترونیک، پایگاه اوریم در صحرای نگب[2] است که در فاصلهٔ حدوداً ۳۰ کیلومتری بئرشبع[3] قرار دارد (Hager, 2010). از نمای بیرونی، این پایگاه دارای «ردیف‌هایی از بشقاب‌های ماهواره‌ای در اندازه‌های مختلف، کانکس‌ها و ساختمان‌های عملیاتی در دو طرف جادهٔ منتهی به پایگاه (جادهٔ ۲۳۳۳) است» (Hager,2010). همچنین تصاویر پایگاه ۳۰ آنتن شنود را نشان می‌دهد که اوریم را به یکی از بزرگ‌ترین پایگاه‌های شنود الکترونیک جهان تبدیل می‌کنند. به‌گفتهٔ هاگر (۲۰۱۰) این پایگاه چند دهه پیش برای نظارت بر ماهواره‌هایی (Intelsat) ساخته شد که تماس‌های تلفنی بین کشورها را هدایت می‌کنند؛ اما بعدها برای پوشش ارتباطات دریایی (Inmarsat) و سپس سایر ماهواره‌های منطقه‌ای گسترش یافت.

یگان ۸۲۰۰ علاوه بر این پایگاه‌ها، پایگاه‌های کوچک‌تری در مناطق مختلف - از جمله در اورا[4]، تل‌آویتال (بلندی‌های جولان)، جبل‌الشیخ و ام هاشیبا در صحرای سینا - در اختیار دارد (Kahana, 2006; Silverstein, 2018, 2016). همچنین گفته می‌شود که در اَفریت - واقع در اورشلیم شرقی - این یگان و آژانس امنیت ملی آمریکا

1. Herzliya
2. Negev desert
3. Beersheba
4. Ora

(NSA) پایگاه مشترکی دارند - یا دست‌کم قبلاً داشته‌اند (Silver-stein, 2014).

و نهایتاً، دولت رژیم صهیونیستی اخیراً در بئرشبع[1] در حال ساخت یک پارک تکنولوژی/سایبری بزرگ به نام پارک تکنولوژی‌های پیشرفته[2] است. این پارک - که به‌گفتهٔ نتانیاهو قرار است تبدیل به «مرکز سایبری نیمکرهٔ غربی» شود - محل تلاقی عناصر بخش‌های خصوصی، آکادمیک، عمومی و نظامی خواهد بود. درواقع، این پارک ترکیبی از دفتر کار و پارک است که نه‌تنها میزبان شرکت‌های بین‌المللی - مثل داچ‌تلکام[3]، آی‌بی‌ام[4]، اوراکل[5]، لاکهید مارتین[6]، ای‌ام‌سی[7] و پی‌پال[8] - خواهد بود، بلکه قرار است میزبان دفتر سایبری ملی[9] جدید دولت و مرکز پژوهش امنیت سایبری[10] دانشگاه بن‌گوریون[11] بئرشبع نیز باشد. تا پایان سال ۲۰۲۰، این پارک محل ستادهای فرماندهی جدید سازمان ضداطلاعات و بخش ارتباطات نیروهای مسلح رژیم صهیونیستی نیز خواهد شد (Reed, 2015).

۳-۲- فرآیند گزینش و آموزش

جذابیت و انگیزش

پیش از انتشار کتاب سنور و سینگر با عنوان «ملت استارت‌آپ»، حتی در رژیم صهیونیستی نیز تقریباً هیچ شناختی از یگان ۸۲۰۰ و خروجی‌های آن در میان عموم وجود نداشت. اما این وضعیت طی چند سال گذشته تغییر کرده است. امروزه متداول است که اعضا و فرماندهان سابق یگان با افتخار و به‌طورعلنی عضویت خود در این

1. Beer Sheva
2. Advanced Technologies Park (ATP)
3. Deutsche Telekom
4. IBM
5. Oracle
6. Lockheed Martin
7. EMC
8. PayPal
9. National Cyber Bureau
10. Cyber Security Research Centre
11. Ben-Gurin University

یگان را اعلام کنند (مثلاً در رزومه‌های کاری[1]، پروفایل‌های لینکدین[2] و غیره). در واقع می‌توان گفت این تغییر رویه تلاشی است از سوی نیروهای مسلح رژیم صهیونیستی برای بازاریابی یگان ۸۲۰۰ در جهت جذب مستعدترین نیروها. به‌این‌ترتیب یگان شهرتی که در دو جنبهٔ اساسی به‌دست آورده است - یعنی میهن‌پرستی/رسالت [ملی]، و منافع مالی/شغلی - در میان نیروهای خود و نیز نیروهای بالقوه ایجاد انگیزه می‌کند.

در جنبهٔ نخست، با عمومی‌شدن و شهرت روزافزون برخی از عملیات‌های این یگان (مثلاً استاکس‌نت)، نیروهای جدید به‌خوبی از نقش محوری آن در تأمین امنیت ملی رژیم صهیونیستی آگاه هستند. اکثر آن‌ها عمیقاً احساس وظیفه‌شناسی و مسئولیت‌پذیری در مورد دفاع از هم‌وطنان، همکاران، دوستان و خانوادهٔ خود دارند. آن‌ها احساس می‌کنند که کارشان در یگان نه تنها معنادار، بلکه تأثیرگذار [و مفید] است (Reed, 2015). این واقعیت که مسئولیتی بزرگ (اینکه زندگی افراد بسیاری در دستان آنهاست) در سن بسیار پایین بر دوش آن‌ها نهاده می‌شود، باعث تشدید این حس در آنان می‌شود (Bar and Shechter, 2015). همچنین وضعیت اضطراری رژیم صهیونیستی و نیروهایش و نزدیکیِ دشمنان و قدرت روزافزون آن‌ها در حوزه سایبری نیز باعث تقویت این انگیزه در نیروهای این یگان می‌شود.

افزون بر میهن‌پرستی، موفقیت بسیاری از خروجی‌های قبلی یگان نیز باعث ایجاد انگیزه در نیروهای جدید می‌شود. رسانه‌ها به‌صورت گسترده به این مسئله پرداخته‌اند که نیروهای تربیت‌شده در این

1. CV
2. LinkedIn profiles

یگان و فرماندهان آن بیش از ۱۰۰۰ شرکت و استارت‌آپ تأسیس کرده‌اند (برای نمونه پالو آلتو نتوورکز[1]، چک‌پوینت[2]، ویز[3]، تیم ۸[4] و غیره). بنابراین، انگیزهٔ مالی روشنی برای یادگیری مهارت‌های فنی لازم جهت ایجاد یک شرکت بزرگ و احیاناً گذار موفق به‌سوی صنایع خصوصی وجود دارد (Rousseau, 2017). با درنظرگرفتن هزینهٔ زیاد تحصیل در مراتب بالاتر آموزشی در رژیم صهیونیستی، اهمیت این انگیزه مالی بیشتر معلوم می‌شود.

همچنین، به علت شهرت یگان به اینکه پذیرفته‌شدن در آن بسیار رقابتی است، سربازان واقفند که هم‌قطارانشان در زمرهٔ باهوش‌ترین استعدادهای کشور هستند. در کشوری که همه یکدیگر را می‌شناسند و تجربهٔ (نظامی) مشترک غالباً اهرمی برای تجارت است، انگیزه‌ای قوی برای به حداکثر رساندن زمان خدمت در یگان ۸۲۰۰ جهت ساختن یک شبکهٔ روابط قدرتمند و ارزشمند وجود دارد (Perman, 2005).

فرآیند غربال‌گری

چنین تصور می‌شود که فرآیند گزینشِ یگان ۸۲۰۰ یکی از سخت‌ترین و محرمانه‌ترین گزینش‌ها در کل نیروهای مسلح رژیم صهیونیستی باشد (به استثنای گزینش خلبان‌های نیروی هوایی). این فرآیند بسیار رقابتی است و یگان برای گزینش باهوش‌ترین نیروها - به‌ویژه در حوزهٔ سایبری - مستقیماً با سایر سرویس‌های اطلاعاتی رقابت می‌کند.

فرآیند گزینش در سنین جوانی آغاز می‌شود. یگان ۸۲۰۰ در واقع

1. Palo Alto Networks
2. Checkpoint
3. Waze
4. Team8

در همان ابتدای دورهٔ دبیرستان شروع به شناسایی نیروهای مستعد بالقوه می‌کند. دانش‌آموزان مستعد در این مقطع معمولاً براساس رتبه، توصیه‌های مدرسه و نیز نظرات مأموران گزینش و جذب نیرو - که برای شناسایی نیروهای آینده‌دار به مدارس سطح کشور اعزام می‌شوند - غربال شده و گزینش می‌شوند.

علاوه‌براین، یگان ۸۲۰۰ به دو طرح دانش‌آموزی دیگر نیز التفات ویژه‌ای دارد. نخست طرح Gvahim (معنای تحت‌اللفظی: بلندی‌ها،تپه‌ها) وزارت آموزش است که کلاس‌های روباتیک و برنامه‌نویسی را در برنامهٔ درسی سال چهارم ۷۰ مدرسه گنجانده است (Estrin, 2017). گروه هدف این برنامه عمدتاً بچه‌های مُرفه‌تر در رژیم صهیونیستی مرکزی است (Reed, 2015).

طرح دوم نیز Magshimim نام دارد و مربوط به پس از فارغ‌التحصیلی از مدرسه است و محوریت آن این است که مهارت‌های کدنویسی و هک‌کردن را به دانش‌آموزان دبیرستانیِ مستعدی که متعلق به مناطق محروم هستند (یعنی مناطق رژیم صهیونیستی جنوبی و شمالی) آموزش دهد. این طرح که دولت و بنیاد راشی[1] (سازمانی خصوصی با هدف کمک به جوانان محروم) بودجهٔ آن را تأمین می‌کنند، از ۳ سال پیش آغاز به کار کرده است و گروه هدف آن نوجوانان بین ۱۶-۱۵ تا ۱۸ ساله است (Estrin, 2017; Reed, 2015). در طول این طرح، نوجوانان «پس از مدرسه دو بار در هفته در کلاس‌های سه‌ساعته حاضر می‌شوند، هفته‌ای ۱۰ ساعت تمرین خانگی مربوط به حوزهٔ سایبری دارند، و سالی دو بار در یک کارگاه شرکت می‌کنند» (Reed, 2015).

1. Rashi Foundation

البتـه ایـن طـرح حالتـی بسـیار رقابتـی داشـته و ورود بـه آن بسـیار دشـوار اسـت. به‌گفتـهٔ ریـد (۲۰۱۵) داوطلبـان - کـه جمعیتـی بالـغ بـر ۲۰۰۰ نفـر در سـال را تشـکیل می‌دهنـد - ابتـدا بایـد در یـک آزمـون آنلایـن شـرکت کننـد؛ آزمونـی کـه شـامل معماهـا و چالش‌هایـی در حـوزه ریاضیـات، منطـق و الگوریتم‌هـا اسـت. بـرای پاسـخ‌دادن بـه ایـن سـؤالات تخصـص کامپیوتـر لازم نیسـت، و داوطلبـان حتـی می‌تواننـد پاسـخ سـؤالات را در اینترنـت جسـتجو کننـد و یـا از والدیـن خـود تقاضـای کمـک کننـد. هـدف از ایـن آزمـون جـذب دانش‌آموزانـی اسـت کـه هراسـی از چالش‌هـا ندارنـد. پـس از ایـن آزمـون اولیـه، مجموعـه‌ای از آزمون‌هـای دشـوارتر برای سـنجش توانایـی داوطلبـان در برنامه‌نویسـی، زبـان و تفکـر خلاقانـه[1] انجـام می‌شـود (Reed, 2015).

نکتـهٔ جالـب توجـه ایـن اسـت کـه یکـی از اهـداف ایـن برنامـه جلوگیری از تبدیل‌شـدن جوانـان بـه هکرهـای سـیاه اسـت. ظاهـراً در ایـن دوره کمـی از مباحـث «اخـلاق سـایبری» نیـز تدریـس می‌شـود و درعین‌حـال، مدرسـان بـر ایـن نکتـه تأکیـد می‌کننـد کـه افـرادی کـه مسـتعد فعالیت‌هـای مجرمانـه باشـند، در ارتـش پذیرفتـه نخواهنـد شـد و بـه احتمـال فـراوان آینـدهٔ شـغلی خـود در حـوزهٔ سـایبری را تباه خواهنـد کرد.

فرآیند گزینش

فرآینـد غربال‌گـری کـه توضیـح داده شـد، در واقـع تنهـا یـک گزینـش مقدماتـی اسـت. گزینـش واقعـی زمانـی به‌طـور رسـمی آغـاز می‌شـود کـه جوانان اسـرائیلی در سـن ۱۷ سـالگی (با برخی از اسـتثناهای دینی و نژادی) بـرای خدمـت اجبـاری فراخوانده می‌شـوند. در ابتدا مجموعـه‌ای از آزمون‌ها و

1. thinking outside the box

مصاحبه‌های استعدادسنجی، روان‌شناسی و پزشکی از اعضای جدید گرفته می‌شود؛ سپس این افراد در یک طبقه‌بندی سلامت و روان‌سنجی (موسوم به نمرهٔ کابا[1]) قرار می‌گیرند که گزینه‌های آن‌ها برای محل گذراندن دوران خدمت اجباری را مشخص می‌کند (Senor and Singer, 2009).

نمرهٔ کابا متشکل از سه بخش مجزا برای مردان و دو بخش برای زنان است (IDF, 2016): DAPAR، TZADAK و TZHAR. این آزمون‌ها، در کنار هم، برای ارزیابی جوانان رژیم صهیونیستی و تقسیم آن‌ها بین یگان‌های مختلف نیروهای مسلح استفاده می‌شود (Rousseau, 2017).

بخش نخست (DAPAR) یک آزمون روان‌سنجی است که طی مصاحبهٔ اولیه با سربازان جدید انجام می‌شود و ۵۰ درصد از نمرهٔ مردان و ۶۰ درصد از نمرهٔ زنان را تشکیل می‌دهد. این آزمون‌ها شبیه آزمون اس‌ای‌تی[2] در آمریکا است و به چند بخش، شامل ریاضیات، درک مطلب، دستورالعمل‌ها، قیاس‌های واژگانی[3] و قیاس‌های شکلی[4] تقسیم می‌شود (Rousseau, 2017).

بخش دوم (TZADAK) مصاحبه‌ای در راستای سنجش جسمی و ذهنی است و شامل کنترل و تأیید اطلاعات سرشماری [شناسنامه‌ای]، بررسی پزشکی و ارزیابی انگیزهٔ پیوستن به یک یگان رزمی می‌شود. این مصاحبه ۳۳ درصد از نمرهٔ کابای مردان را تشکیل می‌دهد اما برای نمرهٔ زنان حساب نمی‌شود.

بخش آخر (TZHAR) که به نمرهٔ آموزش اولیه نیز مشهور است،

۱. واژهٔ اختصاری Kaba که معادل انگلیسی آن quality group به معنای گروه کیفیت است.
۲. اس‌ای‌تی (به انگلیسی SAT) که مخفف کلمات Scholastic Assessment Test به‌معنای آزمون سنجش مدرسی می‌باشد، یکی از دو امتحان استاندارد برای ورود به دانشگاه در آمریکا است که توسط مؤسسه کالج برد مدیریت می‌شود. کالج برد اظهار می‌کند که جمع نمره اس‌ای‌تی با نمره دبیرستان افراد شاخص بسیار بهتری از نمره تنهای دانش‌آموزان برای اجازه ورود به دانشگاه‌ها است.

3. word analogies
4. shape analogies

نشـان می‌دهـد کـه یـک داوطلـب چـه میـزان آمـوزش رسـمی دیـده اسـت. ایـن نمـره ۱۷ درصـد از نمـرهٔ کابـای مـردان و ۴۰ درصـد از نمـرهٔ کابـای زنـان را شـامل می‌شـود (IDF: Nefesh B›Nefesh, 2015).

در مجمـوع، نمـرهٔ کابـا بـر اسـاس مقیاسـی از ۴۱ تـا ۵۶ اسـت. نمره‌های بیـن ۵۲ تـا ۵۶ اجـازه دارنـد کـه افسـر شـوند. در ایـن میـان، یـگان ۸۲۰۰ تأکیـد ویـژه‌ای بـر نمـرهٔ DAPAR دارد و معمـولاً فقـط بـه داوطلبانـی اجـازهٔ ورود می‌دهـد کـه از ۱۰۰ نمـرهٔ ۸۹ یـا بالاتـر را گرفتـه باشـند - چیـزی شـبیه بـه حداقـل نمـرهٔ لازم بـرای ورود بـه دانشـگاه‌های برتـر آمریـکا (IDF: Nefesh B'Nefesh, 2015; in Rousseau, 2017).

پـس از مرحلـهٔ نخسـت، طـی یـک نصـف روز و در مکانـی جداگانـه مصاحبه‌هـا، شبیه‌سـازی‌ها و آزمون‌هـای دیگـری بـرای سـنجش میـزان بلندپـروازی و آینده‌نگـریِ افـراد برگـزار می‌شـود. جالـب آنکـه ایـن مصاحبه‌هـا توسـط افسـران عالی‌رتبـه یـا مسـئول اسـتخدام گرفتـه نمی‌شـود، بلکـه بـه دسـت سـربازان جـوان یـگان ۸۲۰۰ انجـام می‌شـود کـه انگیـزهٔ یافتـن هم‌یگانی‌هـای باکیفیـت در سـر دارنـد (Behar, 2016).

آزمون‌هایـی کـه در ایـن مرحلـه برگـزار می‌شـود نسـبت بـه مرحلـهٔ اول متفـاوت اسـت. به‌گفتـهٔ یکـی از سـربازان ایـن یـگان، آزمون‌هـا بـرای اندازه‌گیـری طیـف وسـیعی از پارامترهـا طراحـی شـده‌اند - از دانـش (ریاضـی، زبـان، کدنویسـی و غیـره)، کنجـکاوی، قاطعیـت، تفکـر تحلیلـی و مهارت‌هـای رهبـری گرفتـه تـا توانایـی آن‌هـا در کار گروهـی، انطبـاق سـریع، تفکر خلاقانـه و یادگیـری سـریع (Choudhury, 2017; Lakin, 2015; Tsipori, 2017).

فرآیند آموزش

نیروهای جدید به‌محض گزینش و عضویت در یگان ۸۲۰۰، به سراغ آموزش نظامی تخصصی می‌روند و به‌جای شرکت در تمرین‌های نظامی سنتی، بیشتر زمان خود را درون ساختمان درمقابل کامپیوترها و در کلاس‌های مختلف صرف می‌کنند (Lakin, 2015). آموزش‌ها در پایگاه یگان ۸۲۰۰ در تقاطع گلیلوت برگزار می‌شود و حدود شش ماه به طول می‌انجامد. بدیهی است که روش‌شناسی و موضوعات موردمطالعه در اختیار عموم گذاشته نمی‌شود؛ اما مصاحبه‌هایی که اخیراً با برخی از خروجی‌های یگان انجام شده، به ما این امکان را می‌دهد که تا حدی با روند آموزش نیروهای جدید آشنا شویم.

طبیعتاً فرآیند آموزش فشرده است و بین ۱۲ تا ۱۸ ساعت از روز زمان می‌برد (Perman, 2005). آریلی[1] اشاره می‌کند که «عضو جدید درون تیم کوچکی قرار می‌گیرد که، از اول صبح تا دیروقت، کارشان مطالعه، طوفان ذهنی، آموزش، تحلیل و حل مسئله است» (Arieli, 2016; in Behar, 2016). در طول این «اردوی پرورش ذهن»، موضوعات بسیار متنوعی مطرح می‌شود – از مهندسی الکترونیک و کدنویسی گرفته تا زبان عربی و ارتباطات (Behar, 2016). به‌علاوه، این نیروها چگونگی تولید و تحلیل اطلاعات، استفاده از شنود الکترونیک، و توسعهٔ تکنیک‌های داده‌کاوی را فرا می‌گیرند و در شبیه‌سازی‌های آموزشی پُرفشار و منظمی نیز شرکت می‌کنند (Darknet Diaries and Sham-ban, 2018).

افسران مسئول آموزش غالباً فقط چند سال بزرگ‌تر از اعضای جدید هستند. این افسران از رویکرد آموزشی موقعیت‌محور[2] (PBS)

1. Arieli
2. Planning by Situations (PBS)

استفاده می‌کنند که محصول مرکز آموزش کامپیوتر مامرام در نیروهای مسلح رژیم صهیونیستی در طول دهۀ ۱۹۸۰ بوده و شبیه رویکرد مطالعۀ موردی مدرسۀ تجاری هاروارد[1] است (Breznitz, 2002; Rousseau, 2017). به گفتۀ برزنیتز[2]، برنامۀ موقعیت‌محور (PBS) «یک رویکرد کل‌گرایانۀ عملگرا به تولید و تدریس مجموعۀ گسسته‌ای از دانش زنجیره‌ای (گام‌به‌گام)» است. روش این برنامه، تمرکز بر ویژگی‌های کیفی و مهارت‌هایی است که دانش‌آموزان برای انجام وظایف آتی خود باید آن‌ها را کسب کنند. از این ویژگی‌های کیفی و مهارتی با عنوان «مؤلفه‌های حرفه‌ای» یاد می‌شود.

به‌منظور اطمینان از تسلط کافیِ نیروهای جدید بر مؤلفه‌های حرفه‌ای، مربیان دوره را حول یک «آزمون نهایی»[3] سامان می‌دهند. این آزمون نهایی در اصل یک پروژۀ پایانی است که به‌منظور شبیه‌سازی و تمرین قابلیت‌ها و مسئولیت‌های لازم فارغ‌التحصیلان طراحی شده است (Breznitz, 2002; Rousseau, 2017). در مورد یگان ۸۲۰۰، مربیان غالباً مسائل فنی و مسائل اطلاعاتی را با هم ترکیب می‌کنند. برای مثال، تیمی از نیروهای جدید باید یک قطعۀ نرم‌افزاری بسازند که پیام دشمن را رمزگشایی کند؛ سپس باید آن را تحلیل کنند و یک اقدام ممکن را پیشنهاد دهند (Perman, 2005; in Rousseau, 2017). پس از این مرحله از آموزش‌ها، سربازان در یگان‌های فرعی زیرمجموعه یگان ۸۲۰۰ تقسیم می‌شوند. گرچه مسئولیت‌های هر یک از این یگان‌های فرعی ممکن است متفاوت باشد، اما مبانی کارشان یکسان باقی می‌ماند.

1. Harvard Business School
2. Breznitz
3. capstone exercise

نیروهای در حال خدمت، نیروهای ذخیره و فارغ‌التحصیلان

دورۀ خدمت سربازی اجباری در رژیم صهیونیستی بین ۳ سال برای مردان و ۲ سال برای زنان نوسان دارد. اما اعضای یگان ۸۲۰۰ غالباً شاهد افزایش خدمت‌شان تا چند سال هستند. درعین‌حال، متوسط زمان خدمت حدود چهار سال است که در طول آن سربازان موظف هستند کل هفته و روزی ۱۸ ساعت کار کنند (Nikolic, 2017).

این سیستم و طول خدمت چهارساله، همواره مجموعۀ قابل‌توجهی از اعضای جدید را در اختیار نیروهای مسلح رژیم صهیونیستی قرار می‌دهد؛ نیروهایی که نرخ گردش سالانۀ جمعیت‌شان حدود ۲۵٪ خواهد بود. فرماندهان یگان این امر را به‌مثابه یک قدرت بزرگ تلقی می‌کنند؛ فرماندهانی که هر سال شاهد «مردان و زنان جدید، جوان، باهوش، پُرانگیزه و مشتاقی هستند که از منظری کاملاً نوین به مسائل می‌نگرند» (Behar, 2016). به‌علاوه، این چرخش دائمی، اعضای یگان را وادار می‌کند تا در طراحی محصولات‌شان دقت زیادی به خرج دهند؛ چراکه وقتی موعد استفاده از محصولات فرا برسد، بیشتر آن‌ها در آنجا نخواهند بود.

اکثر نیروهای یگان با اتمام دورۀ خدمت، به زندگی عادی خود به‌عنوان یک شهروند بازمی‌گردند و حرفه‌های مختلفی مثل کارآفرینی تکنولوژی و سیاست‌مداری را دنبال می‌کنند. بسیاری نیز به سراغ مطالعات دانشگاهی می‌روند. برخی هم ازسوی فرماندهان خود تشویق می‌شوند که درطول خدمت‌شان یک دورۀ فشرده (دو برابر سریع‌تر از معمول) را در علوم کامپیوتری بگذرانند (Nikolic, 2017).

با توجه به ذخیره‌محور بودنِ ساختار ارتش رژیم صهیونیستی، اکثر سربازان قدیمیِ یگان ۸۲۰۰ باید تا رسیدن به اوایل دهه چهل عمرشان، بالغ بر ۳ هفته در سال به‌عنوان نیروی ذخیره به یگان بازگردند (Behar, 2016). این امر سبب ملاقات، همکاری، تبادل افکار و ایده‌ها، و ایجاد پیوندهایی در میان نسل جدید و قدیم یگان می‌شود که بعدها به کار آن می‌آید. در این میان، نیروهای پیشکسوت می‌توانند در جریان آخرین تکنولوژی‌هایی که توسط نیروهای جدیدتر طراحی و توسعه یافته قرار بگیرند و خود را به‌روز کنند.

علاوه بر آموزش‌های سالانه‌ای که باعث به‌روزرسانیِ اطلاعات می‌شود، نیروهای قدیمی یگان به‌واسطهٔ «انجمن/شبکهٔ فارغ‌التحصیلان یگان» ارتباط خود را با یکدیگر حفظ می‌کنند؛ شبکه‌ای که شامل بیش از ۱۵ هزار نفر در سرتاسر جهان است. اگرچه رژیم صهیونیستی دارای تعداد زیادی از این‌گونه انجمن‌های نیروهای قدیمیِ یگان‌های نظامی است، اما انجمن یگان ۸۲۰۰ بخاطر تمرکزی که دارد، در میان این انجمن‌ها برجسته است. برخلاف سایر یگان‌ها که مایل به زنده‌نگه‌داشتن یاد و خاطرهٔ نیروهای قدیمی هستند، یگان ۸۲۰۰ بر استفاده از این گروه برای شبکه‌سازی و توسعهٔ تجاری و نیز کسب استعداد و همکاری تأکید دارد (Kerbs, 2007).

به بیان دقیق‌تر، این انجمن - که چهره‌های برجستهٔ جامعهٔ کارآفرینی رژیم صهیونیستی در رأس آن قرار دارند - به فارغ‌التحصیلان و سربازان قدیمیِ یگان کمک می‌کند که شغلی بیابند، سرمایه‌گذاری کنند یا استعدادهای جدید را برای همکاری به خدمت بگیرند. این امر از طریق بسترهای شبکه‌سازی - مثلاً یک سایت شبکه‌سازی

اینترنتی اختصاصی (شبیه لینکدین) - یا به‌وسیلهٔ یک گروه فیسبوکی محرمانه در میان خود فارغ‌التحصیلان انجام می‌شود (Kane, 2016). این انجمن همچنین تعدادی برنامهٔ خدمات اجتماعی راه‌اندازی کرده است؛ که یکی از آن‌ها شتاب‌دهنده‌ای استارت‌آپی به نام ۸۲۰۰ EISP است. این شتاب‌دهنده زمینه را برای دسترسی استارت‌آپ‌های تازه‌کار به ورک‌شاپ‌هایی که توسط فارغ‌التحصیلان برگزار می‌شود، فراهم می‌کند. یگان ۸۲۰۰ این‌گونه ورک‌شاپ‌ها را برای شناسایی و جذب افراد مستعد برگزار می‌کند و نظارت بر آن‌ها به عهدهٔ اعضای سابق و فعلی یگان است. همچنین این شتاب‌دهنده دسترسی به وقایع انجمن دست‌پرورده‌های یگان ۸۲۰۰ را امکان‌پذیر می‌سازد (EISP 2017; in Rousseau, 2017 8200). نکتهٔ قابل‌توجه این است که اعراب و یهودیان شدیداً ارتدوکس - که اغلب آن‌ها در ارتش خدمت نمی‌کنند یا نمی‌توانند این کار را بکنند - نیز امکان استفاده از این شتاب‌دهنده را دارند (Behar, 2016; Reed, 2015).

۳-۳- فرهنگ درونی

مانند هر فرهنگ دیگری، فرهنگ (کاری) رژیم صهیونیستی نیز دارای ظرایف و پیچیدگی‌هایی است که تنها اسرائیلی‌ها قادر به فهم کامل آن هستند. این امر دربارهٔ فرهنگ حاکم بر یگان ۸۲۰۰ نیز صادق است؛ لذا فهم کامل و دقیق آن چندان آسان نیست. باوجوداین، بر اساس بررسی مصاحبه‌های مختلفی که توسط برخی از دانش‌آموختگان آن صورت گرفته است، (با این هشدار که بررسی ما مبتنی بر یک گفتمان و روایت‌سازی است) می‌توان گفت که

این یگان متضمن و تجسم سه تا از اصلی‌ترین ارزش‌های رژیم صهیونیستی است: Davka، Rosh Gadol، Chutzpah، و Bitzua (Rousseau, 2017).

اصطلاح Chutzpah حدوداً معنای «گستاخی»[1] (Senor and Singer, 2009) یا «وقاحت[2]، پُررویی[3]، بی‌شرمی[4]، دل و جرئت باورنکردنی» است (Rosten, 1968; in Rousseau, 2017). مصداق بارز این ویژگی را می‌توان در گرایش سربازان یگان ۸۲۰۰ به رفتارهای اخلال‌گرانه - و بعضاً هنجارشکنانه - و آمادگی آن‌ها برای این کار مشاهده کرد که اگر معتقد باشند که حرفشان درست است، مقامات بالاتر از خود را به چالش بکشند (Reed, 2015).

ارزش دوم Rosh Gadol [به معنای سَر بزرگ] «نشانهٔ این است که این سَر قادر به گنجاندن تصویری کلان و جامع از امور، مسئولیت‌پذیری و ابتکار عمل، و یا اثبات توانایی رهبری‌کردن بوده و کار خود را نه صرفاً به‌عنوان یک شغل، بلکه به‌منزلهٔ یک رسالت ببینند» (Kordova, 2012). مهم‌ترین نمود این ویژگی را می‌توان در [فرآیند] آموزشِ یگان ۸۲۰۰ مشاهده کرد؛ فرآیندی که تفکر تحلیلی، حس ابتکار و انطباق‌پذیری را شدیداً تشویق و ایجاد می‌کند. درضمن، این سربازان جوان - غالباً بنا به اقتضائات مأموریت‌شان - می‌بایست مسئولیت و مالکیت پروژه‌هایشان را بر عهده بگیرند؛ پروژه‌هایی که شاید حیات دیگران وابسته به آن‌ها باشد.

ارزش سوم [Bitzua] را می‌توان «به انجام رساندن امور» (Senor and Singer, 2009) یا «سرسخت[5]، کاردان[6]، بی‌قرار[7] [به‌معنای مشتاق]، نیش‌دار[8] [به‌معنای دارای زبان و رفتار تیز]، کارا[9]» ترجمه کرد (Wieseltier, 1985; in Rousseau, 2017). در یگان ۸۲۰۰ این واژه به‌معنای

1. audacity
2. gall
3. brazen nerve
4. effrontery
5. crusty
6. resourceful
7. impatient
8. sardonic
9. effective

گرایش به تفکر منعطف، ابتکار، و بداهه‌پردازی برای مقابله با چالش‌هایی است که شاید برخی حل آن را غیرممکن تلقی کنند. این مقابله بعضاً با امکانات بسیارکم و مهلت زمانی اندک صورت می‌گیرد، یا همان‌طورکه یکی از دانش‌آموختگان یگان می‌گوید: «به اعضای یگان آموزش داده می‌شود که چیزی به نام غیرممکن وجود ندارد، درحالی‌که غیرممکن امری موقتی است که با استقامت و پافشاری می‌توان آن را تغییر داد، حتی اگر خود فرماندهٔ یگان بگوید که نمی‌شود» (Kerbs, 2007). این فضا، معمولاً باعث ایجاد سطح مشخصی از رقابتِ هدف‌محور می‌شود؛ رقابتی که از زمان شروع به کار یگان، بر آن سایه افکنده است.

این فضا در اثر ایجاد سطح مشخصی از آزادی عمل و استقلال در یگان تقویت می‌شود؛ به‌عبارت‌دیگر «هیچ‌کس به شما نمی‌گوید که چگونه مأموریت‌های خود را به سرانجام برسانید» (Behar, 2016). درواقع، رویکرد مقامات بالاتر در یگان این است که «مسائل را به شیوهٔ خودتان حل کنید؛ مهم نیست که چقدر زمان می‌بَرد». این نگاه باعث گشوده‌شدن میدان عمل در برابر نیروهای سطوح پایین‌تر در یگان می‌شود. باک[1] (۲۰۱۱) معتقد است که مقامات نسبت به خطاها تساهل دارند (البته تا حدی)، به شرط آنکه موجب درس‌گرفتن از آن خطاها شود.

بنابراین، یگان ۸۲۰۰ توجه ویژه‌ای به نوآوری تکنیکی و استراتژیک داشته و به‌شدت از آن حمایت می‌کند. به‌منظور «حفظ جنون [شور]» (Orpaz, 2015) و پرهیز از بوروکراسی‌زدگی و رضایت به وضع موجود، فرماندهان یگان بخش جداگانه‌ای را تأسیس کرده‌اند که وظیفه‌اش

1. Buck

نوآوری استراتژیک، برگزاری رویدادهای مختلف، و فرآیندهای خودجوش است که از آن جمله می‌توان به هکاتون[1] و نیز رویدادهای موسوم به سوب[2] یا «شنود الکترونیکی خارج از چارچوب (خلاقانه)»[3] اشاره کرد.

هفتهٔ سوب به‌مانند «هفتهٔ خارج از چارچوب» مایکروسافت، یک چیدمان و ساختار استاندارد دارد: در روز نخست، ایده‌ها متبلور می‌شوند. در روز دوم و سوم، محصول مدنظر بدل به یک صورت نوعی می‌شود. روز چهارم، ارائه صورت می‌گیرد و در روز آخر، نتیجه به فرماندهان و رهبران ارشد اطلاعاتی در صنایع های‌تک عرضه می‌شود (Orpaz, 2015). بین سال‌های ۲۰۱۲ تا ۲۰۱۵، مجموعاً ۱۰ رویداد سوب برگزار شد که ۳۰ سرباز در هرکدام شرکت داشتند و بیش از ۸۰ ایدهٔ مختلف ارائه شد. از میان این ایده‌های پیشنهادی، ۱۰ مورد برگزیده شدند و ۵ مورد از آن‌ها تأثیر عمده‌ای بر یگان داشته‌اند (Orpaz, 2015).

سربازان همچنین می‌توانند ایده‌های خود در مورد برخی از عملیات‌ها و یا مسائل بوروکراتیک را به‌طور خودجوش و از طریق سیستمی که در کل یگان گسترده شده است و به‌نحو تهدیدی‌آمیزی نام آن را «اجی‌مجی‌لاترجی» گذاشته‌اند! مطرح کنند[4]. این‌گونه پیشنهادات معمولاً نیروی انسانی لازم برای کار مورد نظر را نیز اعلام می‌کنند. سپس دیگرِ حاضرین در سیستم نیز می‌توانند از طریق توسعهٔ ویژگی‌های فنی محصول و رابط کاربری[5] واکنش نشان دهند (Orpaz, 2015).

---

۱. هکاتون (به انگلیسی: Hackathon) رویدادی است که در آن برنامه‌نویسان رایانه و افراد دیگری که درگیر توسعه نرم‌افزار هستند، از جمله طراحان گرافیکی، طراحان واسط کاربری و مدیران پروژه گرد هم می‌آیند و در توسعه پروژه‌های نرم‌افزاری و گاهی سخت‌افزاری با یکدیگر همکاری می‌کنند.

2. SOOB

3. SIGINT out of the box

۴. آجی مَجی لا تَرَجی (به انگلیسی: Abracadabra) یک ورد است که به‌عنوان کلمه جادویی به کار می‌رود.

۵. رابط کاربری یا میانجی کاربری (به انگلیسی: User Interface) فضایی است که تعامل میان انسان و ماشین در آن رخ می‌دهد. رابط کاربری، بخش دیدنی و قابل لمس یک ابزار است که کاربر مستقیماً با آن سروکار دارد.

بخش چهارم

بحث و تحلیل

بخش چهارم
بحث و تحلیل

پس از تشریح پس‌زمینهٔ تاریخی، سازمانی، فرهنگی و عملیاتی یگان ۸۲۰۰، حال به ارزیابی نقاط قوت و ضعف آن می‌پردازیم.

۴-۱- نقاط قوت

طبق ادبیات نظری موجود، نقاط قوت، ویژگی‌هایی از سازمان هستند که باعث مزیت و برتری آن نسبت به سایر رقبای آن می‌شود. براساس این تعریف نقاط قوت یگان ۸۲۰۰ را می‌توان به این ترتیب برشمرد:

- **منابع انسانی**: همان‌طورکه پیش‌تر نشان دادیم، تعداد کارکنان این یگان حدوداً بین ۵ هزار تا ۱۰ هزار نفر است، که ۵ هزار نفر از آنان همواره درحال انجام وظیفه هستند (Behar, 2016). این رقم پایین‌تر از تعداد کارکنان رقیب آمریکاییِ این یگان - یعنی آژانس امنیت ملی آمریکا (NSA) - است که در سال ۲۰۱۳ حدود ۳۵ الی ۵۵ هزار نیرو در اختیار داشته است (Groll, 2013)، و با ستاد ارتباطات دولت بریتانیا[1] - که در سال ۲۰۱۱/۱۲ تعداد نیروهای آن ۶۱۳۲ نفر بوده است - در یک سطح قرار دارد (Intelligence

1. GCHQ

and Security and Committee of Parliament, 2013). علاوه‌براین، اگر نسبت جمعیت این یگان به کل جمعیت رژیم صهیونیستی (حدود ۸ میلیون نفر) را درنظر بگیریم، میزان چشمگیر آن بی‌درنگ مشخص می‌شود. از نظر مزیت رقابتی، این بدنهٔ نیرویی نسبتاً گسترده به یگان امکان می‌دهد که توانمندی‌های خود را تخصصی کرده و در حوزه‌های مختلفی (مثل داده‌کاوی، هوش مصنوعی و غیره) توسعه دهد، و نیز طیف وسیعی از فعالیت‌ها و مأموریت‌ها (همچون عملیات‌های سایبری تهاجمی، رمزگشایی و غیره) را دنبال کند. اثرات محتمل ناشی از «صرفه به مقیاس»[1] نیز می‌توانند مورد بهره‌برداری قرار بگیرند.

• **زیرساخت‌ها و امکانات مالی**: دربارهٔ میزان دقیق منابع یگان ۸۲۰۰ نیز با اطلاعات چندانی در دسترس نیست. اما اگر اندازه و پیچیدگی برخی از عملیات‌های آن (مانند استاکس‌نت، که از چهار نقطهٔ آسیب‌پذیر صفر روزه[2] استفاده کرد) درنظر گرفته شود، می‌توان پذیرفت که این یگان دارای منابع مالی عظیمی است. این بودجهٔ وافر، در کنار منابع انسانی غنی که پیش‌تر اشاره کردیم، یگان را قادر می‌سازد که با تکنیک‌هایی از قبیل هدایت عملیات‌های متعدد - که بعضاً با بودجه‌ای بسیار محدود و در سطوح بسیار پیچیده اجرا می‌شود -، بتواند به یک مزیت رقابتی نائل شود. همچنین، این منابع مالی به یگان اجازه می‌دهد که برنامهٔ تحقیق و توسعهٔ (R&D) خودش را - مشخصاً بواسطهٔ یگان

۱. صرفه به مقیاس یا مزیت مقیاس (به انگلیسی: Economies of scale) مفهومی در اقتصاد خُرد است که به کسب مزیت کاهش هزینه در اثر افزایش حجم تولید اشاره دارد. صرفه به مقیاس به معنای آن است که با افزایش حجم تولید، هزینه متوسط تولید هر واحد کالا کاهش می‌یابد. دلایل متعددی برای این مسئله وجود دارد که شامل مواردی همچون: کسب تخفیف در خرید به دلیل حجم بالای خرید، افزایش تجربه و یادگیری کارکنان، کسب منابع مالی بیشتر، سرشکن شدن هزینه‌های بازاریابی در بازارهای وسیع‌تر و بهبود فناوری تولید است.

۲. حمله صفر روزه یا حمله روز صفر (به انگلیسی: Zero-day attack) یک حمله یا تهدید رایانه‌ای است که از یک آسیب‌پذیری در یک نرم‌افزار کاربردی که تا پیش از آن ناشناخته بوده است، استفاده می‌کند. این بدان معناست که توسعه‌دهندگان برای رفع آسیب‌پذیری صفر روز فرصت داشته‌اند.

۸۱ - پیش ببرد و برخی از پیشرفته‌ترین سلاح‌ها و نرم‌افزارهای تکنولوژیک جهان را طراحی کند. نهایتاً آنکه، این سطح از منابع انسانی و مالی یگان را قادر می‌سازد تا نه تنها یک زیرساخت گسترده (با تکنولوژی‌های پیشرفته‌ای از آنتن‌ها و ماهواره‌ها) و پایگاه‌های بزرگ‌مقیاسی (مثل پایگاه اوریم به‌عنوان یکی از بزرگ‌ترین پایگاه‌های شنود الکترونیک جهان) را حفظ و اداره کند، بلکه همچنین امکان سرمایه‌گذاری بر روی زیرساخت‌های نوین را نیز برای آن فراهم می‌کند.

• **توانمندی‌ها و دانش عملی**: طی دهه‌های گذشته، یگان ۸۲۰۰ علاوه‌بر تکنولوژی، امکانات سایبری و اطلاعاتی قابل‌توجهی را توسعه داده است. به بیان دقیق، یگان اکنون دارای یک حافظه و دانش عملی و نهادی است که کشورهای بسیار کمی قادر به رقابت با آن هستند. این توانمندی بواسطهٔ سال‌ها آموزش به نیروهای جدید منتقل می‌شود (با نرخ ریزش ۲۵ درصدی). این دانش که با تکمیل مأموریت‌ها و پیگیری نوآوری‌های یگان پیوسته استوارتر می‌گردد، یکی از نقاط قوت کلیدی یگان در حفظ حاشیهٔ رقابتی نسبت به دشمنان و دوستان است.

• **فرهنگ درونی**: نقطهٔ قوت بعدی، فرهنگ درونی این یگان است. درواقع، یگان ۸۲۰۰ از طریق یک طراحی هوشمندانه - یعنی تیم‌های کوچک و جداگانه، با میزان زیادی از خودمختاری و یک سلسله‌مراتب افقی - روحیهٔ کاریِ کاملاً اسرائیلی را فضای خود حاکم کرده است؛ روحیه‌ای که علی‌رغم پراکندگیِ نسبی و بداهه‌بودن، باعث شکل‌گیری نوآوری مؤثری در عملیات‌ها می‌شود. به‌علاوه،

وجـود یـک سـاختار قـدرت برابری‌طلـب و صمیمیتـی کـه از پـی آن می‌آیـد، کمـک شـایانی بـه غلبـه بـر انـواع سـوگیری‌های موجـود در جامعـهٔ شـهری - مثـل جنسـیت، سـن و تجربـه - می‌کنـد. همچنیـن، واگـذاری مسـئولیت بزرگـی بـه اعضـا در سـنین جوانـی، بـه آن‌هـا کمـک می‌کنـد تـا پیـش از رویارویـی بـا واقعیـات زندگـی حرفـه‌ای و آکادمیـک، (به‌ویـژه زنـان (Asher-Dotan et al., 2018)) صاحـب بلـوغ، تجربـه و اعتمادبه‌نفـس شـوند.

• **بِرنـد یـگان۸۲۰۰ و فرآینـد (پیشـا) غربال‌گـری**: یکـی از نقـاط قـوت یـگان ۸۲۰۰ کـه در ایـن پژوهـش به آن اشـاره شـد، توانایـیِ آن در شناسـایی، جـذب و (تـا حـدودی) حفـظ نیروهـای کارآمـد و بااسـتعداد اسـت. ایـن یـگان بـه ۲ دلیـل همـواره بـه منبـع گسـترده‌ای از نیـروی انسـانیِ ماهـر دسترسـی دارد: اولاً بـه دلیـل شـهرت و برنـد معتبرِ ایـن یـگان؛ و ثانیـاً بخاطـر فرآیندهـای غربال‌گـری و گزینشـی (و مراحـلِ مقـدم بـر اینهـا). بِرنـد ایـن یـگان طـی سـال‌ها بـا دقـت و از طریـق اقدامـات نوآورانـهٔ دانش‌آموختـگان، علنی‌کـردنِ عملیات‌هـای برجسـته، تبلیغـات و گفتمان‌سـازی دولـت، و مصاحبـه بـا دانش‌آموختگانـی کـه اسـتارت‌آپ‌های خصوصـیِ خودشـان را بـا موفقیـت تأسـیس کـرده بوده‌انـد، سـاخته و پرداختـه شـده اسـت. ایـن شـهرت به‌نوبهٔ‌خـود آگاهـی گسـترده‌ای در مـورد یـگان ایجـاد کـرده و تصویـری از آن سـاخته اسـت کـه بـرای نیروهـای جـوان و ماهـر بسـیار جـذاب اسـت. درعین‌حـال، فرآیندهـای غربال‌گـری و گزینـش بـه یـگان ایـن امـکان را می‌دهـد تـا اسـتعدادهای جـوان را - هم‌زمـان بـا آغـاز فرآینـد توسـعه و پـرورش توانایی‌هـا و مهارت‌هـای آن‌هـا کـه حتـی قبـل از پیوسـتن

به یگان شروع شده است - شناسایی و ردیابی کند. همچنین این فرآیند باعث اطمینان از این مسئله می‌شود که مسئولان عضوگیری قادر به گزینش داوطلبینی هستند که با نیازهای یگان سازگار باشند.

• **حلقه‌های [افراد] نخبه و سطح‌بالا**: سرانجام، یکی از مهم‌ترین نقاط قوت یگان ۸۲۰۰، محیطی است که یگان به آن دسترسی دارد و درون آن عمل می‌کند؛ به‌ویژه وحدت و انسجامِ حاکم بر جامعهٔ تکنولوژی‌های های‌تک رژیم صهیونیستی و همکاری نزدیکی که بین بخش‌های اقتصادی، نظامی، دولتی و آکادمیک برقرار است (برای نمونه، پارک سایبری بئرشبع). این محیطْ حلقه‌های نخبگانیِ متعددی را شکل می‌دهد که هم یگان و هم سایر بخش‌های درگیر در این فضا از آن سود می‌برند. برای نمونه، حلقهٔ متخصصان سایبریِ کشور به‌واسطهٔ دورهٔ مشترکی که در یگان ۸۲۰۰ می‌گذارنند و یا سایر موقعیت‌ها - مثلاً [تشکیل] انجمن دانش‌آموختگان یگان -، ارتباط تنگاتنگی با یکدیگر دارند. این امر نه تنها باعث اعتمادسازی [در بین این افراد] می‌شود، بلکه فرآیند عضوگیری را تسهیل کرده و تشریفات زائد را به حداقل می‌رساند. در واقع دانش‌آموختگان یگان به‌عنوان واسطهٔ همکاری‌های آتی بین یگان و شرکت‌های خصوصی عمل می‌کنند. مضافاً اینکه یگان ۸۲۰۰ (و در سطحی کلان‌تر کل کشور رژیم صهیونیستی) نیز - به‌صورت مستقیم و غیرمستقیم - از پژوهش و توسعهٔ تکنولوژی‌های نوین در حوزهٔ دفاع و امنیت سایبری - که توسط شرکایش صورت می‌گیرد - سود می‌برد.

۴-۲- نقاط ضعف

نقـاط ضعـف یعنـی بخش‌هایـی از ویژگی‌هـای درونـی یـک سـازمان کـه آن را در مقایسـه بـا سـایر سـازمان‌ها تضعیـف می‌کننـد. بـر ایـن اسـاس نقـاط ضعـف یـگان ۸۲۰۰ را می‌تـوان مـوارد زیـر دانسـت:

- **مناقشـات سیاسـی**: در سـال‌های اخیـر یـگان ۸۲۰۰ به‌علـت برخـی از فعالیت‌هـای خـود، کم‌وبیـش بدنـام و حاشیه‌سـاز شـده اسـت. ایـن امـر به‌ویـژه در سـال ۲۰۱۴ زبانـزد شـد کـه ۴۳ عضـو نیروهـای ذخیـرۀ ایـن یـگان در نامـه‌ای سرگشـاده و امضاشـده، تحت‌نظـر گرفتـن [و شـنود] «غیراخلاقـی» فلسـطینی‌هایی را کـه هیـچ ارتباطـی بـا فعالیت‌هـای خشـونت‌آمیز نداشـته‌اند را محکـوم کردنـد (Williams, 2014). این‌گونـه افشـاگری‌ها و رسـوایی‌ها نـه تنهـا بـرای خـود یـگان ۸۲۰۰، بلکـه به‌طورکلـی بـرای کشـور رژیـم صهیونیسـتی عواقبـی منفـی در پـی دارنـد. به‌عنـوان نمونـه می‌تـوان بـه دوره‌ای اشـاره کـرد کـه ایـن یـگان بیشـتر از همیشـه زیـر ذره‌بیـن کنشـگران داخلـی و خارجـی قـرار گرفتـه بـود و خطـرِ فاش‌شـدنِ برخـی از فعالیت‌هـا و روش‌هـای کاریِ آن کامـلاً حـس می‌شـد. علاوه‌برایـن، این‌گونـه اتفاقـات باعـث افزایـش خطـر اختـلاف عقیـده در میـان نیروهـای رده‌پاییـنِ یـگان و بوجودآمـدن زمینـه‌ای بـرای افشـاگری در آینـده می‌شـود. ایـن افشـاگری‌ها می‌توانـد وجهـۀ رژیـم صهیونیسـتی را لکـه‌دار و فشـار بین‌المللـی را بیشـتر کنـد.
- **زیـاده‌روی در بوروکراسـی**: همان‌طورکـه بالاتـر در بخش‌هـای قبلـی اشـاره کردیـم، یـگان ۸۲۰۰ نسـبت بـه روزهـای اولیـۀ شـکل‌گیری تحولاتـی اساسـی را از سـر گذرانـده و بـدل بـه یکـی از بزرگ‌تریـن

یگان‌های نیروهای مسلح رژیم صهیونیستی شده است. به‌عبارت دقیق‌تر، یگان ۸۲۰۰ علی‌رغم طراحی غیرمتمرکز فعلیِ خود، تا حدودی مستعد زیاده‌روی در بوروکراسی است؛ البته طبیعتاً در مورد هر سازمان دیگری با این ابعاد، چنین احتمالی وجود دارد. گرچه مسلماً چنین چیزی فی‌نفسه نقطه‌ضعف نیست، اما سیستماتیک‌شدنِ بیش از حدِ فرآیندهای داخلی، ممکن است باعث سرکوبِ نوآوریِ ایده‌آل و باکیفیتی بشود که در این یگان به چشم می‌خورد. یگان ۸۲۰۰ به این خطر واقف است و پیشاپیش با تأسیس «دپارتمان قانون حفظ جنون [شور]»[1] و فعالیت‌های مختلف این سازمان، به این مسئله واکنش نشان داده است (Or-paz, 2015).

• **عضوگیری نخبه‌محور و طردکننده**: به زعم جانسون و همکاران (۲۰۱۷)، بخش عمدهٔ عضوگیری یگان ۸۲۰۰ از ناحیهٔ ثروتمندتر و تحصیل‌کرده‌تر تل‌آویو (محل کار تعدادی از دانش‌آموختگان یگان ۸۲۰۰ در صنایع های‌تک) و نیز دبیرستان‌های نخبه‌پرور (مثلاً لیادا[2]، دبیرستان دانشگاهی عبری نیمه‌خصوصی در اورشلیم) صورت می‌گیرد. این سوگیری و عدم توازن ممکن است در اثر عوامل مختلفی از جمله تأثیرات شبکه‌سازی‌ها و همچنین دسترسی بهترِ عده‌ای از داوطلبان به دوره‌هایی باشد که مجموعه مهارت‌های لازم برای [موفقیت در] فرآیند گزینش را آموزش می‌دهند. یک ویژگی دیگر - که البته ممکن است فی‌نفسه نقطه‌ضعف به حساب نیاید - این است که چنین رویه‌ای احتمالاً باعث می‌شود که فرآیند عضوگیریِ این یگان - برخلاف استراتژی‌های

1. Department of the Law for Preserving Madness
2. Leyada

برنامه‌های اختصاصیِ این کار (از جمله طرح Magshimim) - به طیف کوچکی از جمعیت کشور محدود شود و در نتیجه، یگان از به‌خدمت‌گرفتنِ نیروهای «کم شانس» ولی مستعد باز می‌ماند. همچنین، این خطر وجود دارد که گروه خاصی از نخبگان در فرآیند عضوگیری شانس بیشتری داشته باشند (برای مثال فرزندان دانش‌آموختگان ممتاز). این وضعیت - در میان‌مدت و بلندمدت - نابرابری‌های موجود در میان مردم (برای نمونه ممنوعیت خدمت اعراب اسرائیلی) و مناطق مختلف کشور رژیم صهیونیستی (مثل تل‌آویو در مقابل رژیم صهیونیستی مرکزی) را تقویت کرده و بر ثبات درونی کشور اثر منفی می‌گذارد.

• **محیط غیرسنتی**: مسئلهٔ دیگر، مشکلات مربوط به گذار از فعالیت‌های نظامی به [سایر] فعالیت‌های حرفه‌ای است. برخی از دانش‌آموختگان یگان ۸۲۰۰ پس از گذراندن چند سال در این یگان، سازگاری با محیط‌های حرفه‌ای، هنجارها، سلسله‌مراتب و ساختارهای سنتی‌تر را دشوار یافته‌اند. گرچه چنین چیزی نقطه‌ضعفی برای خود یگان نیست، اما موضوعی است که می‌تواند برای موفقیت دانش‌آموختگان آن و به‌طورکلی اقتصاد رژیم صهیونیستی تبعاتی را به همراه داشته باشد.

• **شهرت و توانمندی‌های روزافزون دشمنان**: دشمنان (و متحدان) فراوان رژیم صهیونیستی در سراسر جهان در حال گسترش توانمندی‌های سایبری تهاجمی و تدافعی خود هستند. این وضعیت، طبیعتاً منجر به شکل‌گیری نوعی رقابت تسلیحاتی خواهد شد - از نظر پیچیدگی و نیز حجم تسلیحات - که احتمالاً

هزینهٔ فعالیت‌های یگان را افزایش می‌دهد. شهرت یگان ۸۲۰۰ باعث بغرنج‌ترشدنِ این وضعیت خواهد شد؛ زیرا آن را بدل به هدفی بیش‌ازپیش رؤیت‌پذیر و جذاب برای حملات آتی می‌سازد.

• **بی‌ثباتی و نظارت سیاسی**: با وجود جو سیاسی موجود در رژیم صهیونیستی و جنجال‌های مختلف پیرامون این یگان (برای نمونه، ممنوع‌الخروج‌ها، گروه NSO و غیره)، تشدید نظارت، تفحص یا مقررات‌گذاری برای فعالیت‌های یگان می‌تواند فرآیندهای عملیاتی آن را مختل کند. البته شدت هر اختلال بستگی به موقعیت دارد. برای مثال، پیشنهاد تجدیدنظر در ساختار یگان از سوی کمیسیونی که در سال ۲۰۰۴ پس از جنگ عراق تشکیل شده بود، می‌توانست برخی از فعالیت‌های رایج یگان و پیوندهایش با یگان‌های نظامی دیگر را تضعیف و جامعهٔ اطلاعاتی شدیداً متوازن رژیم صهیونیستی را بی‌ثبات کند.

بخش پنجم

نتیجه‌گیری و توصیه‌ها

بخش پنجم

نتیجه‌گیری و توصیه‌ها

در مقام نتیجه‌گیری و با توجه به پس‌زمینه و تحلیل‌های فوق، می‌توان توصیه‌هایی کلی برای هر سازمان یا برنامه‌ای که خواهان درس‌آموزی از یگان ۸۲۰۰ است، ارائه کرد. مهم‌ترین این توصیه‌ها از این قرارند:

- نسبت به تخصیص منابع انسانی و مالی کافی و نیز زیرساخت‌های های‌تک به برنامهٔ مدنظر اطمینان حاصل کنید.
- از انتقال منظم و پیوستهٔ دانش عملی و تجربیات حمایت کنید. این امر نه تنها شامل تبادل عمودی این موارد در طول آموزش نیروهای جدید است، بلکه به اشتراک‌گذاری افقی آن‌ها میان نیروهای جدید و ذخیره را نیز در بر می‌گیرد. این امر به‌ویژه در مورد صنایع تکنولوژیک که بسیار سریع پیشرفت می‌کنند مطرح است؛ جایی که عوامل دولتی و صنایع های‌تک گاهی اوقات از نظر زمانی با یکدیگر همگام نیستند.
- فرهنگ کارآفرینی و نوآوری را درون سازمان تقویت کنید. گرچه چنین کاری در یک ساختار سلسله‌مراتبی بعضاً دشوار است، اما - برای مثال - می‌توان از طریق یک ساختار نامتمرکز و پروژه/

مأموریت‌محور (با تیم‌های کوچک، منعطف و خودمختار)، یا سلسله‌مراتب مسطحی که در آن «کارکرد» مهم‌تر از «مرتبه» باشد، و یا ایجاد منظم چالش برای اعضا، و سایر روش‌ها، این فرهنگ را تقویت نمود.

- پیوندهای خود با بخش خصوصی را تقویت کنید. این مورد به دلایل مختلفی، از جمله دلایل تکنولوژیک و اقتصادی، حیاتی است. همان‌طورکه قبلاً اشاره شد، در این عرصهٔ تکنولوژیک، اقدامات شبکه‌ای (مثلاً از طریق انجمن دانش‌آموختگان یا صفحات فیسبوک) برای به‌روز ماندن و نوآوری‌های بیشتر مهم هستند. به‌علاوه، شراکت‌ها و کارآموزی‌ها تجربهٔ حرفه‌ای مرتبط و دسته‌اولی را در اختیار اعضای جدید قرار می‌دهد و در عین حال باعث اعتمادسازی و تسهیل در فرآیند استخدام آن‌ها می‌شود.
- جذابیت حرفه‌ای و عمومی برنامه‌ها را هم برای اعضای جدید و هم کارمندان آینده افزایش دهید. این امر مخصوصاً در کشورهایی که هزینه-فرصتِ آموزش‌های جایگزین نسبتاً پایین است، اهمیت دارد. از جهات کاربردی، برای مثال می‌توان به توسعهٔ گواهی‌نامه‌ها یا مدارک مشترک و معتبر، و برنامه‌های دانشگاهی فشرده برای افسران یا حتی بورسیه‌های نظامی برای نیروهای جدید به‌منظور مطالعات دانشگاهی فکر نمود. همچنین، تجربهٔ منحصربه‌فرد و دسته‌اولی را که نیروهای جدید از این برنامه‌ها کسب می‌کنند باید قویاً برجسته و به‌عنوان نکته‌ای کلیدی مطرح نمود.
- آگاهی عمومی نسبت به برنامه و موفقیت‌های آن را گسترش

دهید تا ضمن ارسال یک سیگنال قوی (مثلاً درخصوص موضوع بازدارندگی و مشروعیت)، بهترین افراد ممکن را جذب کنید. این امر با ایجاد یک برند قابل‌شناسایی و نیز شهرت و هویت مستحکم اتفاق می‌افتد. برای مثال، این کار می‌تواند با افزایش نمود عمومی برنامه، به‌ویژه در نمایشگاه‌های شغلی یا دانشجویی، در طی رویداد هکاتون یا بازدید از برنامه‌های بعد از مدرسه، محقق شود. تبلیغات هدفمند یا استفاده از اپلیکیشن‌های نظامی برای تبلیغ برنامه‌ها نیز می‌توانند گزینه‌های دیگر باشند. به‌علاوه، با توجه به شهرتی که کل حوزهٔ سایبری در اذهان عمومی دارد، می‌توان کارهای قابل‌توجهی در مورد توضیح نقش و فعالیت‌های برنامه‌ها انجام داد تا ترس‌ها را از میان برد.

بخش ششم

فهرست اصطلاحات

بخش ششم

فهرست اصطلاحات

- **مسئلهٔ انتساب**: یعنی دشواری مربوط به تشخیص قطعی مقصر/مرتکب یک حملهٔ سایبری. شناسایی حمله‌کنندگان دشوارتر است، زیرا آن‌ها قادر به مخفی‌کردن ردپای خود، اجرای حملات سایبری فریب‌دهنده یا مقصر جلوه‌دادن کنشگران دیگر هستند (Hay Newman, 2016).

- **توانمندی‌های سایبری**: تجهیزات، تکنیک‌ها یا برنامه‌های کامپیوتری که برای متلاشی‌کردن/فرسوده‌کردن[1]، اختلال یا خرابکاری و دستکاری در اطلاعات، و سیستم‌ها و شبکه‌های اطلاعات در فضای سایبری یا از طریق آن طراحی شده‌اند (Brangetto and Veenendaal, 2016).

- **هک**: ورود بدون مجوز به یک سیستم (Ghernaouti-Hélie, 2013, p. 433)

- **بدافزار**: نرم‌افزار بدکارکردی که می‌تواند شکل یک ویروس، کرم یا اسب تروا را به خود بگیرد (Collins and McCombie, 2012, p. 81)

- **شنود الکترونیک**: جمع‌آوری اطلاعات از طریق ردگیری سیگنال‌های ارتباطاتی یا الکترونیک.

1. degradation

۶-۱- علائم اختصاری

اَمان (AMAN)	دفتر ضداطلاعات ارتش
ATP	پارک تکنولوژی‌های پیشرفته
GCHQ	ستاد ارتباطات حکومتی
IDF	نیروهای مسلح رژیم صهیونیستی
ISNU	یگان ملی شنود الکترونیک رژیم صهیونیستی
MAMRAM	مرکز سیستم‌های کامپیوتری و اطلاعاتی
NSA	آژانس امنیت ملی
OSINT	منابع اطلاعاتی آزاد
SIGINT	شنود الکترونیک

منابع

(1) Agranat Commission of Inquiry, 1974. Interim Report.

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

(3) 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

(4) 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/

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

(6) 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

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

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

(9) 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.

(10) 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

(11) 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

(12) 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

(13) 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/

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

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

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

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

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

(19) 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

(20) 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.

(21) 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/

(22) 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/

(23) 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/

(24) 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/

(25) 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

(26) 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/

(27) 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/

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

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

(30) 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/

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

(32) 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/

(33) Intelligence and Security, Committee of Parliament, 2013. Intelligence

and Security Committee of Parliament Annual Report 2012–2013.

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

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

(36) 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/

(37) Kaspesky Lab, 2015. The Duqu 2.0 Technical Details.

(38) 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

(39) 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

(40) 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

(41) 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/

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

(43) 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

(44) 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

(45) 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.

(46) 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

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

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

(49) Ravid, B., 2012. Officials: Israel Outsources Monitoring of Palestinian

Media After IDF Lapse [WWW Document]. Haaretz. URL https://www.haaretz.com/1.517821

(50) 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/

(51) 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

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

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

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

(55) 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-cyber-attacks-against-iran.html

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

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

(58) Shamir, E., 2005. Computer Science and Technology in Israel, 1950–1980 [WWW Document]. Rutherford J. URL http://www.rutherfordjour-

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

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

(61) 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/

(62) 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/

(63) 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/

(64) 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/

(65) 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

(66) 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/

(67) 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

(68) 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

(69) 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

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

(71) 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

(72) 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

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

csri.majazi.ir

حوزه فضای مجازی به اندازه انقلاب اسلامی اهمیت دارد. این فضا مثل یک رودخانه پر از آب و خروشان است که می آید و دائماً هم بر آب آن افزوده و خروشان تر می شود. اگر ما بر این رودخانه تدبیر کنیم و برنامه داشته باشیم، زه‌کشی کنیم و هدایت کنیم این رودخانه را تا به سد بریزد، می‌شود فرصت. اگر رهایش کنیم و برنامه‌ای برای آن نداشته باشیم می‌شود یک تهدید.

سید حسن

csri.majazi.ir