INVESTIGATIVE SERIES

# How the CIA, Mossad and “the Epstein Network” are Exploiting Mass Shootings to Create an Orwellian Nightmare

Israel’s Mossad and infamous Unit 8200 are partnering with the CIA and US tech firms to create an Orwellian pre-crime nightmare.

BY **WHITNEY WEBB** · SEPTEMBER 6, 2019 · 40 MINUTE READ


*This article was originally published on MintPress News.*

Following the arrest and subsequent death in prison of alleged child sex trafficker Jeffrey Epstein, a little-known Israeli tech company began to receive increased publicity, but for all the wrong reasons. Not long after Epstein’s arrest, and his relationships and finances came under scrutiny, it was revealed that the Israeli company Carbyne911 had received substantial funding from Jeffrey Epstein as well as Epstein’s close associate and former

substantial funding from Jeffrey Epstein as well as Epstein's close associate and former Prime Minister of Israel Ehud Barak, and Silicon Valley venture capitalist and prominent Trump backer Peter Thiel.

Carbyne911, or simply Carbyne, develops call-handling and identification capabilities for emergency response services in countries around the world, including the United States, where it has already been implemented in several U.S. counties and has partnered with major U.S. tech companies like Google. It specifically markets its product as a way of mitigating mass shootings in the United States without having to change existing U.S. gun laws.

Yet, Carbyne is no ordinary tech company, as it is deeply connected to the elite Israeli military intelligence division, Unit 8200, whose "alumni" often go on to create tech companies — Carbyne among them — that frequently maintain their ties to Israeli intelligence and, according to Israeli media reports and former employees, often "blur the line" between their service to Israel's defense/intelligence apparatus and their commercial activity. As this report will reveal, Carbyne is but one of several Israeli tech companies marketing themselves as a technological solution to mass shootings that has direct ties to Israeli intelligence agencies.

In each case, these companies' products are built in such a way that they can easily be used to illegally surveil the governments, institutions and civilians that use them, a troubling fact given Unit 8200's documented prowess in surveillance as a means of obtaining blackmail and Israel's history of using tech companies to aggressively spy on the U.S. government. This is further compounded by the fact that Unit 8200-linked tech companies have previously received U.S. government contracts to place "backdoors" into the U.S.' entire telecommunications system as well as into the popular products of major American tech companies including Google, Microsoft and Facebook, many of whose key managers and executives are now former Unit 8200 officers.

Israeli Prime Minister Benjamin Netanyahu has made it no secret that placing Unit 8200 members in top positions in multinational tech companies is a "deliberate policy" meant to ensure Israel's role as the dominant global "cyber power", while also combating non-violent boycott movements targeting Israel's violations of international law and stifling the United Nations' criticisms of Israeli government policy and military operations abroad.

As Jeffrey Epstein's links to intelligence in both the United States and Israel — the subject of a recent four-part series exclusive to *MintPress* — began to be revealed in full, his financing of Carbyne came under scrutiny, particularly for the company's deep ties to

Israeli intelligence as well as to certain Americans with known connections to U.S. intelligence. Ehud Barak's own role as both financier and chairman of Carbyne has also added to that concern, given his long history of involvement in covert intelligence operations for Israel and his long-standing ties to Israeli military intelligence.

Another funder of Carbyne, Peter Thiel, has his own company that, like Carbyne, is set to profit from the Trump administration's proposed hi-tech solutions to mass shootings. Indeed, after the recent shooting in El Paso, Texas, President Trump — who received political donations from and has been advised by Thiel following his election — asked tech companies to "detect mass shooters before they strike," a service already perfected by Thiel's company Palantir, which has developed "pre-crime software" already in use throughout the country. Palantir is also a contractor for the U.S. intelligence community and also has a branch based in Israel.

Perhaps most disturbing of all, whatever technological solution is adopted by the Trump administration, it is set to use a controversial database first developed as part of a secretive U.S. government program that involved notorious Iran-Contra figures like Oliver North as a means of tracking and flagging potential American dissidents for increased surveillance and detention in the event of a vaguely defined "national emergency."

As this report will reveal, this database — often referred to as "Main Core" — was created with the involvement of Israeli intelligence and Israel remained involved years after it was developed, and potentially to the present. It was also used by at least one former CIA official on President Reagan's National Security Council to blackmail members of Congress, Congressional staffers and journalists, among others.

Given recent reports on the Trump administration's plan to create a new government agency to use "advanced technology" to identify "neurobehavioral signs" of "someone headed toward a violent explosive act" using data collected by consumer electronic devices, the picture painted by the technology currently being promoted and implemented under the guise of "keeping Americans safe" is deeply Orwellian. In fact, it points directly to the genesis of a far-reaching surveillance state far more extensive than anything yet seen in American history and it is being jointly developed by individuals connected to both American and Israeli intelligence.

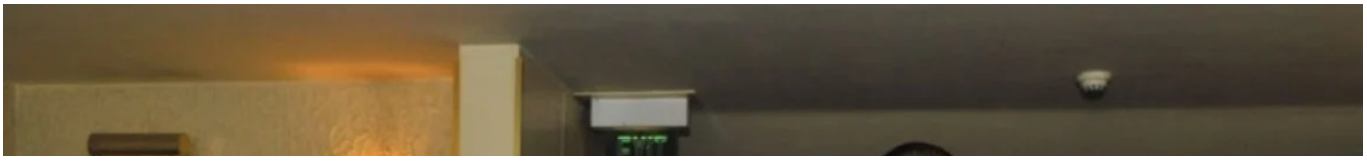
# Demystifying Carbyne

Carbyne911, which will be referred to simply as Carbyne in this report, is an Israeli tech-startup that promises to revolutionize how calls are handled by emergency service providers, as well as by governments, corporations and educational institutions. Not long after it was founded in 2014 by veterans of Israeli military intelligence, Carbyne began to be specifically marketed as a solution to mass shootings in the United States that goes "beyond the gun debate" and improves the "intelligence that armed emergency responders receive before entering an armed shooter situation" by providing video-streaming and acoustic input from civilian smartphones and other devices connected to the Carbyne network.

Prior to Jeffrey Epstein's arrest in July, Carbyne had been receiving high praise from U.S. and Israeli media, with *Fox News* hailing the company's services as the answer to the U.S.' "aging 911 systems" and the *Jerusalem Post* writing that the company's platform offers "hi-tech protection to social workers and school principals." Other reports claimed that Carbyne's services result in "a 65% reduction in time-to-dispatch."

Carbyne's call-handling/crisis management platform has already been implemented in several U.S. counties and the company has offices not only in the U.S. but also in Mexico, Ukraine and Israel. Carbyne's expansion to more emergency service provider networks in the U.S. is likely, given that federal legislation seeks to offer grants to upgrade 911 call centers throughout the country with the very technology of which Carbyne is the leading provider. One of the main lobby groups promoting this legislation, the National Emergency Number Association (NENA), has a "strong relationship" with Carbyne, according to Carbyne's website. In addition, Carbyne has also begun marketing its platformfor non-emergency calls to governments, educational institutions and corporations.

Yet, what seemed like the inevitability of Carbyne's widespread adoption in the U.S. hit a snag following the recent arrest and subsequent death of sex trafficker and pedophile Jeffrey Epstein, who exploited underage girls for the purpose of obtaining "blackmail" on the rich and poweful, an operation that had clear ties to intelligence. Epstein, after his first arrest and light sentence for soliciting sex from a minor in 2007, was tapped by former Israeli Prime Minister and former head of Israeli military intelligence Ehud Barak, to become a key financial backer of Carbyne.




Ehud Barak, center, poses with Carbyne co-founders Alex Dizengof, Amir Elichai and Lital Leshem. Photo | Yossi Seliger

As a result of increased scrutiny of Epstein's business activities and his ties to Israel, particularly to Barak, Epstein's connection to Carbyne was revealed and extensively reported on by the independent media outlet *Narativ*, whose exposé on Carbyne revealed not only some of the key intelligence connections of the start-up company but also how the architecture of Carbyne's product itself raises "serious privacy concerns."

*MintPress* detailed many of Carbyne's main intelligence connections in Part III of the investigative series "Inside the Jeffrey Epstein Scandal: Too Big to Fail." In addition to Barak — former Israeli prime minister and former head of Israeli military intelligence — serving as Carbyne's chairman and a key financer, the company's executive team are all former members of Israeli intelligence, including the elite military intelligence unit, Unit 8200, which is often compared to the U.S. National Security Agency (NSA).

Carbyne's current CEO, Amir Elichai, served in Unit 8200 and tapped former Unit 8200 commander and current board member of AIPAC Pinchas Buchris to serve as the company's director and on its board. In addition to Elichai, another Carbyne co-founder, Lital Leshem, also served in Unit 8200 and later worked for Israeli private spy company Black Cube. The only Carbyne co-founder that didn't serve in Unit 8200 is Alex Dizengof, who previously worked for Israel's Prime Minister's office.

As *MintPress* noted in a past report detailing Israeli military intelligence's deep ties to

American tech giant Microsoft, Unit 8200 is an elite unit of the Israeli Intelligence corps that is part of the IDF's Directorate of Military Intelligence and is involved mainly in signal intelligence (i.e., surveillance), cyberwarfare and code decryption. It is frequently described as the Israeli equivalent of the NSA and Peter Roberts, senior research fellow at Britain's Royal United Services Institute, characterized the unit in an interview with the *Financial Times* as "probably the foremost technical intelligence agency in the world and stand[ing] on a par with the NSA in everything except scale."

Notably, the NSA and Unit 8200 have collaborated on numerous projects, most infamously on the Stuxnet virus as well as the Duqu malware. In addition, the NSA is known to work with veterans of Unit 8200 in the private sector, such as when the NSA hired two Israeli companies, to create backdoors into all the major U.S. telecommunications systems and major tech companies, including Facebook, Microsoft and Google. Both of those companies, Verint and Narus, have top executives with ties to Israeli intelligence and one of those companies, Verint (formerly Comverse Infosys), has a history of aggressively spying on U.S. government facilities. Unit 8200 is also known for spying on civilians in the occupied Palestinian territories for "coercion purposes" — i.e., gathering info for blackmail — and also for spying on Palestinian-Americans via an intelligence-sharing agreement with the NSA.

Unlike many other Unit 8200-linked start-ups, Carbyne also boasts several tie-ins to the Trump administration, including Palantir founder and Trump ally Peter Thiel — another investor in Carbyne. In addition, Carbyne's board of advisers includes former Palantir employee Trae Stephens, who was a member of the Trump transition team, as well as former Secretary of Homeland Security Michael Chertoff. Trump donor and New York real-estate developer Eliot Tawill is also onCarbyne's board, alongside Ehud Barak and Pinchas Buchris.

Yet, privacy concerns with Carbyne go beyond the company's ties to Israeli intelligence and U.S. intelligence contractors like Peter Thiel. For instance, Carbyne's smartphone app extracts the following information from the phones on which it is installed:

> **"Device location, video live-streamed from the smartphone to the call center, text messages in a two-way chat window, any data from a user's phone if they have the Carbyne app and ESInet, and any information that comes over a data link, which**

**Carbyne opens in case the caller's voice link drops out." (emphasis added)**

According to Carbyne's website, this same information can also be obtained from any smartphone, even if it does not have Carbyne's app installed, if that phone calls a 911 call center that uses Carbyne or merely any other number connected to Carbyne's network.


Carbyne gathers data points from users' phones as well as a myriad of other web-connected devices.

Carbyne is a Next-Generation 9-11 (NG911) platform and the explicit goal of NG911 is for all 911 systems nationwide to become interconnected. Thus, even if Carbyne is not used by all 911 call centers using an NG911 platform, Carbyne will ostensibly have access to the data used by all emergency service providers and devices connected to those networks. This guiding principle of NG911 also makes it likely that one platform will be favored at the

federal level to foster such interconnectivity and, given that it has already been adopted by several counties and has ties to the Trump administration, Carbyne is the logical choice.

Another cause for concern is how other countries have used platforms like Carbyne, which were first marketed as emergency response tools, for the purpose of mass surveillance. *Narativ* noted the following in its investigation of Carbyne:

> **"In May, Human Rights Watch revealed Chinese authorities use a platform not unlike Carbyne to illegally surveil Uyghurs. China's Integrated Joint Operations Platform brings in a much bigger data-set and sources of video, which includes an app on people's phones. Like Carbyne, the platform was designed to report emergencies. Chinese authorities have turned it into a tool of mass surveillance.**
>
> **Human Rights Watch reverse-engineered the app. The group discovered the app automatically profiles a user under 36 "person types" including "followers of Six Lines" which is the term used to identify Uyghurs. Another term refers to "Hajj," the annual Islamic pilgrimage to Mecca. The app monitors every aspect of a user's life, including personal conversations [and] power usage, and tracks a user's movement."**

Such technology is currently used by Israeli military intelligence and Israel's domestic intelligence agency Shin Bet to justify "pre-crime" detentions of Palestinians in the occupied West Bank. As will be noted in greater detail later in this report, Palestinians' comments on social media are tracked by artificial intelligence algorithms that flag them for indefinite detention if they write social media posts that contain "tripwire" phrases such as "the sword of Allah."

Carbyne's platform has its own "pre-crime" elements, such as it's a Records component

Carbyne's platform has its own "pre-crime" elements, such as it's c-Records component, which stores and analyzes information on past calls and events that pass through its network. This information "enables decision makers to accurately analyze the **past and present behavior of their callers**, react accordingly, and in time **predict future patterns**." (emphasis added)

Concerns have recently been raised that "pre-crime" technology may soon become more widely adopted in the U.S., after President Trump stated that one of his planned solutions to mass shootings in the wake of the recent tragedy in El Paso was for big tech companies to detect potential shooters before they strike.

# Israeli intelligence, Blackmail and Silicon Valley

Though many of the individuals involved in funding or managing Carbyne have proven ties to intelligence, a closer look into several of these players reveals even deeper connections to both Israeli and U.S. intelligence.

One of Carbyne's clearest connections to Israeli intelligence is through its chairman and one of its funders, Ehud Barak. Though Barak is best known for being a former prime minister of Israel, he is also a former minister of defense and the former head of Israeli military intelligence. He oversaw Unit 8200's operations, as well as other units of Israeli military intelligence, in all three of those positions. For most of his military and later political career, Barak has been closely associated with covert operations.

Prior to the public scrutiny of Barak's relationship to Jeffrey Epstein, following the latter's arrest this past July and subsequent death, Barak had come under fire for his ties to disgraced film mogul Harvey Weinstein. Indeed, it was Ehud Barak who put Weinstein in contact with the Israeli private intelligence outfit Black Cube, which employs former Mossad agents and Israeli military intelligence operatives, as Weinstein sought to intimidate the women who had accused him of sexual assault and sexual harassment. Former Mossad director Meir Dagan led Black Cube's board until his death in 2016 and Carbyne co-founder Lital Leshem is Black Cube's former director of marketing.

After Barak put him in contact with Black Cube's leadership, Weinstein, according to *The*

*New Yorker*, used the private spy firm to "'target,' or collect information on, dozens of individuals, and compile psychological profiles that sometimes focused on their personal or sexual histories." In addition, *The New Yorker* noted that "Weinstein monitored the progress of the investigations personally" and "also enlisted former employees from his film enterprises to join in the effort, collecting names and placing calls that, according to some sources who received them, felt intimidating."

Yet, more recently, it has been Barak's close relationship to Epstein that has raised eyebrows and opened him up to political attacks from his rivals. Epstein and Barak were first introduced by former Israeli Prime Minister Shimon Peres in 2002, a time when Epstein's pedophile blackmail and sex trafficking operation was in full swing.

Barak was a frequent visitor to Epstein's residences in New York, so often that *The Daily Beast* reported that numerous residents of an apartment building linked to Epstein "had seen Barak in the building multiple times over the last few years, and nearly half a dozen more described running into his security detail," adding that "the building is majority-owned by Epstein's younger brother, Mark, and has been tied to the financier's alleged New York trafficking ring." Specifically, several apartments in the building were "being used to house underage girls from South America, Europe and the former Soviet Union," according to a former bookkeeper employed by one of Epstein's main procurers of underage girls, Jean Luc Brunel.

Barak is also known to have spent the night at one of Epstein's residences at least once, was photographed leaving Epstein's residence as recently as 2016, and has admitted to visiting Epstein's island, which has sported nicknames including "Pedo Island," "Lolita Island" and "Orgy Island." In 2004, Barak received $2.5 million from Leslie Wexner's Wexner Foundation, where Epstein was a trustee as well as one of the foundation's top donors, officially for unspecified "consulting services" and "research" on the foundation's behalf.

In 2015, Barak formed a limited partnership company in Israel for the explicit purpose of investing in Carbyne (then known as Reporty) and invested millions of dollars in the company, quickly becoming a major shareholder and subsequently the company's public face and the chairman of its board. At least $1 million of the money invested in this Barak-created company that was later used to invest in Carbyne came from the Southern Trust Company, which was owned by Jeffrey Epstein.

In July, Bloomberg reported that Epstein's Southern Trust Company is identified in U.S.

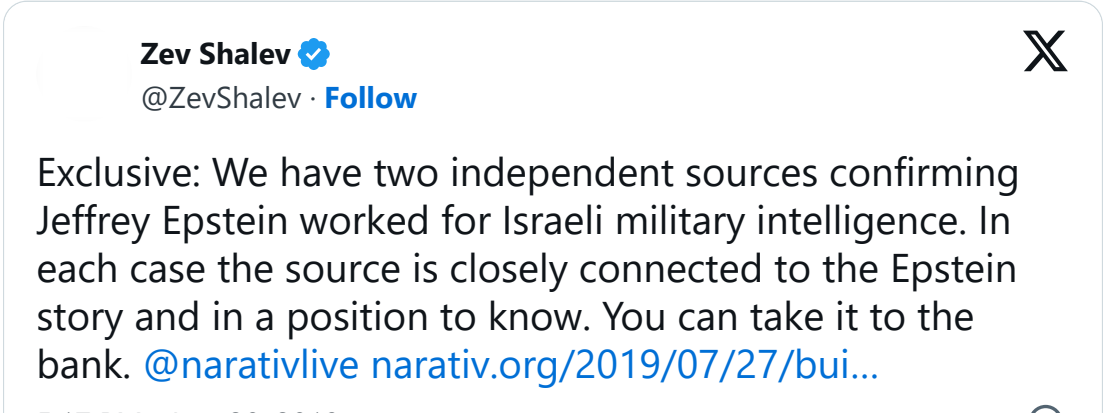
Virgin Islands filings as "a DNA database and data mining" company. Given Carbyne's clear potential for data-mining and civilian profiling, Epstein's investment in Carbyne using this specific company suggests that Carbyne's investors have long been aware of this little advertised aspect of Carbyne's product.

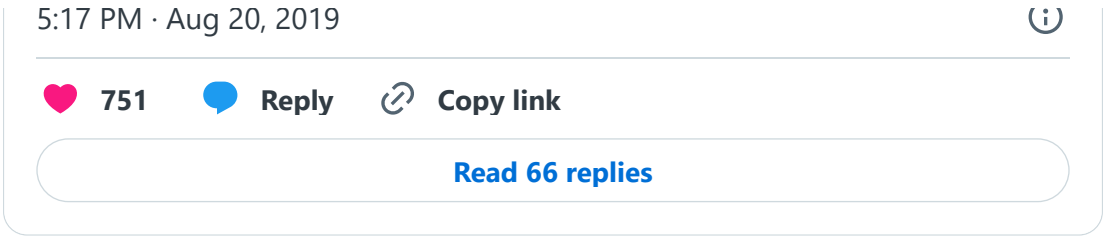
In a statement to the Israeli newspaper *Haaretz*, Barak asserted:

> **"I saw the business opportunity and registered a partnership in my control in Israel. A small number of people I know invest in it…Since these are private investments, it wouldn't be proper or right for me to expose the investors' details."**

However, Barak later admitted that Epstein had been one of the investors.

*MintPress'* recent series on the Jeffrey Epstein scandal noted in detail Epstein's ties to CIA/Mossad intelligence assets, such as Adnan Khashoggi; CIA front companies, such as Southern Air Transport; and organized crime, through his close association with Leslie Wexner. In addition, Epstein's long-time "girlfriend" and alleged madam, Ghislaine Maxwell, has family links to Israeli intelligencethrough her father, Robert Maxwell. While it appears that Epstein may have been working for more than one intelligence agency, Zev Shalev, former executive producer for *CBS News* and journalist at *Narativ*, recently stated that he had independently confirmed with two unconnected sources "closely connected to the Epstein story and in a position to know" that Epstein had "worked for Israeli military intelligence."






Notably, Epstein, who was known for his interest in obtaining blackmail through the sexual abuse of the underaged girls he exploited, also claimed to have "damaging information" on prominent figures in Silicon Valley. In a conversation last year with *New York Times* reporter James Stewart, Epstein claimed to have "potentially damaging or embarrassing" information on Silicon Valley's elite and told Stewart that these top figures in the American tech industry "were hedonistic and regular users of recreational drugs." Epstein also told Stewart that he had "witnessed prominent tech figures taking drugs and arranging for sex" and claimed to know "details about their supposed sexual proclivities."

In the lead-up to his recent arrest, Jeffrey Epstein appeared to have been attempting to rebrand as a "tech investor," as he had done interviews with several journalists including Stewart about technology investing in the months before he was hit with federal sex trafficking charges.

Jessica Lessin, editor-in-chief of *The Information*, told *Business Insider* that a journalist working for *The Information* had interviewed Epstein a month before his recent arrest because "he was believed to be an investor in venture capital funds." However, Lessin claimed that the interview was not "newsworthy" and said the site had no plans to publish its contents. *Business Insider* claimed thatthe way the interviews with Epstein had been arranged "suggests that someone in Silicon Valley may have been trying to help Epstein connect with reporters."

Though it is unknown exactly which Silicon Valley figures were most connected to Epstein and which tech executives were potentially being blackmailed by Epstein, it is known that Epstein associated with several prominent tech executives, including Google co-founder Sergey Brin, Facebook co-founder Mark Zuckerberg, Tesla CEO Elon Musk, Microsoft co-founder Bill Gates, and LinkedIn co-founder Reid Hoffman.

Last year, Epstein claimed to be advising Tesla and Elon Musk, who had been previously photographed with Epstein's alleged madam Ghislaine Maxwell. A few years ago, Epstein also attended a dinner hosted by LinkedIn's Reid Hoffman, where Musk had allegedly introduced Epstein to Mark Zuckerberg. Google's Sergey Brin is known to have attended a dinner hosted by Epstein at his New York residence where Donald Trump was also in

dinner hosted by Epstein at his New York residence where Donald Trump was also in attendance.

Elon Musk with Epstein’s alleged madam Ghislaine Maxwell at an Oscars after-party on March 2, 2014. Kevin Mazur | VF14

These associations suggest that the person in Silicon Valley who was trying to boost Epstein’s image as a tech investor before his arrest may have been Peter Thiel, whose Founders Fund had also invested in Carbyne. Thiel was an early investor in Facebook and is still on its board, connecting him to Zuckerberg; he is also a funder of Elon Musk’s SpaceX and a former colleague of Musk’s through PayPal. In addition, Thiel has ties to Reid Hoffman and both Thiel and Hoffman are prominent backers of Facebook.

It is unknown whether Epstein’s “damaging information” and apparent blackmail on notable individuals in the American technology industry were used to advance the objectives of Carbyne, which recently partnered with tech giants Google and Cisco Systems — and, more broadly, the expansion of Israeli intelligence-linked tech companies into the American tech sector, particularly through the acquisition of Israeli tech start-ups

linked to Unit 8200 by major U.S. tech companies.

The latter seems increasingly likely given that the father of Ghislaine Maxwell — one of Epstein's chief co-conspirators in his intelligence-linked sexual blackmail operation involving minors — was a Mossad operative who helped sell softwarethat had been bugged by Israeli intelligence to government agencies and sensitive facilities around the world, including in the United States.

As will be noted later in this report, Israel's Prime Minister Benjamin Netanyahu — to whom all of Israel's intelligence agencies answer by virtue of his position — has stated on more than one occasion that the acquisition of Israeli intelligence-linked start-ups by foreign tech giants, especially in Silicon Valley, is a current and "deliberate policy" of the state of Israel.

# Carbyne's ties to U.S. intelligence

While Epstein and Barak are the two financiers of Carbyne whose ties to intelligence are clearest, another funder of Carbyne, Peter Thiel, has ties to U.S. intelligence and a history of investing in other companies founded by former members of Unit 8200. Thiel co-founded and still owns a controlling stake in the company Palantir, which was initially funded with a $2 million investment from the CIA's venture capital fund In-Q-Tel and quickly thereafter became a contractor for the CIA.

After the success of its contract with the CIA, Palantir became a contractor for a variety of federal agencies, including the FBI, the Defense Intelligence Agency (DIA), the National Security Agency (NSA), the Department of Homeland Security(DHS) and the military's Special Operations Command, among others. Last year, it won a contract to create a new battlefield intelligence system for the U.S. Army. Palantir is also in demand for its "pre-crime technology," which has been used by several U.S. police departments. According to the *Guardian*, "Palantir tracks everyone from potential terrorist suspects to corporate fraudsters, child traffickers and what they refer to as 'subversives'... it is all done using prediction."

Thiel has gained attention in recent years for his support of President Trump and for becoming an adviser to Trump following the 2016 election, when he was "a major force in the transition," according to *Politico*, and "helped fill positions in the Trump administration

the transition," according to *Politico*, and "helped fill positions in the Trump administration with former staff." One of those former staffers was Trae Stephens, who is also on Carbyne's board of advisers. Thiel also has business ties to Trump's son-in-law and influential adviser, Jared Kushner, as well as to Kushner's brother Josh. A senior Trump campaign aide told *Politico* in 2017 that "Thiel is immensely powerful within the administration through his connection to Jared."

Thiel has also backed some prominent Israeli tech start-ups connected to Unit 8200, such as BillGuard, which Thiel funded along with former Google CEO Eric Schmidt and other investors. BillGuard was founded by Raphael Ouzan, a former officer in Unit 8200, who serves on the board of directors of Start-Up Nation Central (SUNC) alongside neoconservative American hedge fund manager Paul Singer, neoconservative political operative and adviser Dan Senor, and Terry Kassel, who works for Singer at his hedge fund, Elliott Management.

Peter Thiel greets Netanyahu during a 2017 meeting in Israel. Photo | Israel PM

SUNC is an organization founded by Paul Singer, who has donated heavily to both President Trump and Israeli Prime Minister Netanyahu. Since it was founded in 2012, SUNC has sought to integrate Unit 8200-connected Israeli tech start-ups into foreign

SUNC has sought to integrate Unit 8200-connected Israeli tech start-ups into foreign companies, primarily American companies, and has helped oversee the shift of thousands of high-paying tech jobs from the U.S. to Israel.

Another Carbyne-connected individual worth noting is the former head of the Department of Homeland Security, Michael Chertoff, who serves on Carbyne's board of advisers. In addition to Chertoff's ties to DHS, Chertoff's company, The Chertoff Group, employees several prominent former members of the U.S. intelligence community as principals, including Michael Hayden, former director of the CIA and former director of the NSA; and Charles Allen, former assistant director of Central Intelligence for Collection at the CIA, who worked at the agency for over 40 years.

The Chertoff Group has a long-standing and lucrative contract with the company OSI Systems, which produces full-body scanners and markets itself as a solution to mass shootings and crisis events, not unlike Carbyne. While Chertoff's company was advising OSI Systems, Chertoff went on a media blitz to promote the widespread use of the machines produced by OSI Systems and even called on Congress to "fund a large-scale deployment of next-generation systems." Chertoff did not disclose his conflict of interest while publicly promoting OSI's full-body scanners.

Some have also alleged that Chertoff's mother, Livia Eisen, had links to Israeli intelligence. According to her 1998 obituary, cited by both researcher/author Christopher Bollyn and journalist Jonathan Cook, Eisen participated in the Mossad operation code-named "Magic Carpet" while working for Israel's El Al Airlines. Both Bollyn and Cook have suggested that Eisen's participation in this covert Israeli intelligence operation strongly indicates that she had ties to the Mossad.

# Melding into Silicon Valley

Beyond its troubling connections to Silicon Valley oligarchs, Israeli military intelligence and the U.S.-military industrial complex, Carbyne's recent partnerships with two specific technology companies — Google and Cisco Systems — raise even more red flags.

Carbyne announced its partnership with Cisco Systems this past April, with the latter announcing that it would begin "aligning its unified call manager with Carbyne's call-handling platform, allowing emergency call centers to collect data from both 911 callers

and **nearby government-owned IoT [Internet of Things] devices**." A report on the partnership published by *Government Technology* magazine stated that "Carbyne's platform will be integrated into Cisco Kinetic for Cities, an IoT data platform that shares data across community infrastructure, smart city solutions, applications and connected devices." The report also noted that "Carbyne will also be the only 911 solution in the Cisco Marketplace."

As part of the partnership, Carbyne's President of North American Operations Paul Tatro told *Government Technology* that the Carbyne platform would combine the data it obtains from smartphones and other Carbyne-connected devices with "what's available through nearby Cisco-connected road cameras, roadside sensors, smart streetlamps, smart parking meters or other devices." Tatro further asserted that "Carbyne can also analyze data that's being collected by Cisco IoT devices ... and alert 911 automatically, without any person making a phone call, if there appears to be a worthy problem," and expressed his view that soon most emergency calls will not be made by human beings but "by smart cars, telematics or other smart city devices."

A few months after partnering with Cisco Systems, Carbyne announced its partnership with Google on July 10, just three days after Carbyne funder Jeffrey Epstein was arrested in New York on federal sex trafficking charges. Carbyne's press release of the partnership described how the company and Google would be teaming up in Mexico "to offer advanced mobile location to emergency communications centers (ECCs) throughout Mexico" following the conclusion of a successful four-week pilot program between Carbyne and Google in the Central American nation.

Google Executive Chairman Eric Schmidt meets Netanyahu at his Jerusalem office. Israel PM | YouTube

The press release also stated:

> **"Carbyne will provide Google's Android ELS (Emergency Location Service) in real time from emergency calls made on AndroidTM devices. Deployment for any ECC in the country won't require any integration, with Carbyne providing numerous options for connection to their secure ELS Gateway once an ECC is approved. The Carbyne automated platform, requiring no human interaction, has the potential to save thousands of lives each year throughout Mexico."**

The reason Carybne's partnerships with Cisco Systems and Google are significant lies in the role that Cisco and former Google CEO Eric Schmidt have played in the creation of a controversial "incubator" for Israeli tech start-ups with deep ties to Israeli military intelligence, American neoconservative donor Paul Singer, and the U.S.' National Security Agency (NSA).

This company, called Team8, is an Israeli company-creation platform whose CEO and co-founder is Nadav Zafrir, former commander of Unit 8200. Two of the company's other three co-founders are also "alumni" of Unit 8200. Among Team8's top investors is Schmidt, the former CEO of Google, who also joined Peter Thiel in funding the Unit 8200-linked BillGuard, as well as major tech companies including Cisco Systems and Microsoft.

Last year, Team8 controversially hired the former head of the NSA and U.S. Cyber Command, Retired Admiral Mike Rogers, and Zafrir stated that his interest in hiring Rogers was that Rogers would be "instrumental in helping strategize" Team8's expansion in the United States. Jake Williams, a veteran of NSA's Tailored Access Operations (TAO) hacking unit, told *CyberScoop*:

> **"Rogers is not being brought into this role because of his technical experience. …It's purely because of his knowledge of classified operations and his ability to influence many in the U.S. government and private-sector contractors."**

Team8 has also been heavily promoted by Start-Up Nation Central (SUNC). SUNC prominently features Team8 and Zafrir on the cybersecurity section of its website and also sponsored a talk by Zafrir and an Israeli government economist at the World Economic Forum, often referred to as "Davos," that was attended personally by Paul Singer.

SUNC itself has deep ties to Israeli military intelligence, with former Unit 8200 officer Raphael Ouzan serving on its board of directors. Another example of SUNC-Unit 8200 ties can be seen with Inbal Arieli, who served as SUNC's Vice President of Strategic Partnerships from 2014 to 2017 and continues to serve as a senior adviser to the organization. Arieli, a former lieutenant in Unit 8200, is the founder and head of the 8200 Entrepreneurship and Innovation Support Program (EISP), which was the first start-up accelerator in Israel aimed at harnessing "the vast network and entrepreneurial DNA of [Unit] 8200 alumni" and is currently one of the top company accelerators in Israel, alongside Team8. Arieli was the top executive at 8200 EISP while working at SUNC and several other top SUNC staffers are also connected to Israeli military intelligence.

Thus, Google and Cisco's connections to Team8 suggests that their partnerships with another Israeli military intelligence-connected firm like Carbyne is a deepening of those two companies' links to the growing bi-national security state that is uniting key players in the U.S. military-industrial complex and Israeli intelligence.

# Mossad-backed Panic Buttons, coming to a school near you

Carbyne is hardly the only Israeli intelligence-linked tech company marketing itself in the United States as a solution to mass shootings. Another Israeli start-up, known as Gabriel, was founded in 2016 in response to a shooting in Tel Aviv and the Pulse Nightclub shooting in the United States, which took place just days apart.

Created by Israeli-American Yoni Sherizen and Israeli citizen Asaf Adler, Gabriel is similar to Carbyne in the sense that elements of its crisis response platform require installation on civilian smartphones as well as devices used by crisis responders. The main difference is that Gabriel also installs one or a series of physical "panic buttons," depending on the size of the building to be secured, that also double as video and audio communication devices connected to the Gabriel network.

As with Carbyne, the ties between Gabriel and Israeli intelligence are obvious. Indeed, Gabriel's four-person advisory board includes Ram Ben-Barak, former deputy director of the Mossad and former director-general of Israel's intelligence ministry; Yohanan Danino, former chief of police for the state of Israel; and Kobi Mor, former director of overseas missions for the Israeli intelligence agency Shin Bet. The only American on the advisory board is Ryan Petty, the father of a Parkland shooting victim and friend of former Florida Governor Rick Scott.

Gabriel's only disclosed funder is U.S.-based MassChallenge, a start-up accelerator non-profit. Gabriel is funded by MassChallenge's Israel branch, which was opened six months prior to Gabriel's creation and is partnered with the Israeli government and the Kraft Group. The Kraft Group is managed by Robert Kraft, who is currently embroiled in a prostitution scandal and is also a close friend of President Trump.

Notably, one of MassChallenge Israel's featured experts is Wendy Singer, the executive director of SUNC, the organization created and funded byneoconservative Trump backer Paul Singer with the explicit purpose of promoting Israel's tech start-ups and their integration into foreign, chiefly American, businesses. As was noted in a recent *MintPress* report on SUNC, Wendy Singer is the sister of neoconservative political operative Dan Senor, who founded the now-defunct Foreign Policy Initiative with Robert Kagan and Bill Kristol, and was previously the director of AIPAC's Israel office for 16 years.

Gabriel's founders have been quite upfront about the fact that the uptick in shootings in the U.S. has greatly aided their company's growth and success. Last November, Sherizen told *The Jerusalem Post* that new mass shootings in the U.S. not only increased

U.S. demand for his company's product but also were opportunities to show the effectiveness of Gabriel's approach:

> **"Unfortunately every month there seems to be another high-profile event of this nature. After the Vegas shooting, we were able to show [that] our system would have managed to identify the location of the shooter much quicker."**

*The Jerusalem Post* noted that Gabriel is set to make considerable profits if concern over mass shootings continues to build in the U.S., writing:

> **"With more than 475,000 soft targets across the US and amid increasing security fears, the potential market for Gabriel is huge. The company could gain revenues of almost $1 billion if only 10% of soft targets were to invest around $20,000 in its alert systems."**

Sherizen told *the Jerusalem Post*:

> **"Our starter kit costs $10,000. Depending on the size and makeup of the community building, it would cost between $20-30,000 to fully outfit the location. We have made it very affordable. This is a game-changer for the lock-down and active shooter drills that are now a standard part of any child's upbringing in the States."**

# Much more than just a start-up

While it is certainly possible that numerous former officials and commanders of elite Israeli intelligence agencies may have no ulterior motive in advising or founding technology start-up companies, it is worth pointing out that top figures in Israel's military intelligence agencies and the Mossad don't see it that way.

Last March, Israeli media outlet *Calcalist Tech* published a report entitled "Israel Blurs the Line Between Defense Apparatus and Local Cybersecurity Hub," which noted that "since 2012, cyber-related and intelligence projects that were previously carried out in-house in the Israeli military and Israel's main intelligence arms are transferred to companies that in some cases **were built for this exact purpose**." (emphasis added)

The article notes that beginning in 2012, Israel's intelligence and military intelligence agencies began to outsource "activities that were previously managed in-house, with **a focus on software and cyber technologies**." (emphasis added)

It continues:

> **"In some cases, managers of development projects in the Israeli military and intelligence arms were encouraged to form their own companies, which then took over the project,' an Israeli venture capitalist familiar with the matter told Calcalist Tech."**

Notably, *Calcalist Tech* states that the controversial company Black Cube was created this way and that Black Cube had been contracted, and is likely still contracted, by Israel's Ministry of Defense. The private security agency Black Cube is known to have two separate divisions for corporations and governments. The firm was recently

caught attempting to undermine the Iran nuclear deal — then also a top political objective of Israeli Prime Minister Benjamin Netanyahu — by attempting to obtain information on the "financial or sexual impropriety" (i.e., blackmail) of top U.S. officials involved in drafting the accord. *NBC News* notedlast year that "Black Cube's political work frequently intersects with Israel's foreign policy priorities." As previously mentioned, one of Carbyne's co-founders — Lital Leshem, also a veteran of Unit 8200 — worked for Black Cube prior to starting Carbyne.


The entrance to Black Cube's offices on the 26th floor of a Tel Aviv high rise, Feb. 8, 2019. Raphael Satter | AP

One of the main companies profiled in the *Calcalist Tech* report appeared to be a front for Israeli intelligence, as its registered owner was found not to exist: even high-level employees at the company had never heard of him; his registered addresses were for nonexistent locations in Israel's capital of Tel Aviv; and the three people with that name in Tel Aviv denied any association with the business.

This company — which *Calcalist Tech* was unable to name after the Israeli military censor determined that doing so could negatively impact Israeli "national security" — was deliberately created to service the Israeli military and Israeli intelligence. It is also

"focused on **cyber technologies** with expertise in research and development of advanced products and applications suitable for defense and **commercial** entities." (emphases added) In addition, the company's management consists largely of "veterans of Israeli military technology units."

Notably, a former employee of this company told *Calcalist Tech* that "crossing the lines between military service and employment at the commercial outfit was 'commonplace' while he was working at the company."

It's not exactly clear why Israel's military intelligence and other intelligence agencies decided to begin outsourcing its operations in 2012, though *Calcalist Tech* suggests the reasoning was related to the difference in wages between the private sector and the public sector, with pay being much higher in the former. However, it is notable that 2012 was also the year that Paul Singer — together with Netanyahu's long-time economic adviser and former chair of the Israeli National Economic Council, Eugene Kandel — decided to create Start-Up Nation Central.

As *MintPress* noted earlier this year, SUNC was founded as part of a deliberate Israeli government effort to counter the nonviolent Boycott, Divest and Sanctions (BDS) movement and to make Israel the dominant global "cyber power." This policy is aimed at increasing Israel's diplomatic power and specifically undermining BDS as well as the United Nations, which has repeatedly condemned Israel's government for war crimes and violations of international law in relation to the Palestinians.

Last year, Netanyahu was asked by *Fox News* host Mark Levin whether the large growth seen in recent years in Israel's technology sector, specifically tech start-ups, was part of Netanyahu's plan. Netanyahu responded, "That's very much my plan ... It's a very deliberate policy." He later added that "Israel had technology because the military, especially military intelligence, produced a lot of capabilities. These incredibly gifted young men and women who come out of the military or the Mossad, they want to start their start-ups."

Netanyahu again outlined this policy at the 2019 Cybertech Conference in Tel Aviv, where he stated that Israel's emergence as one of the top five "cyber powers" had "required allowing this combination of military intelligence, academia and industry to converge in one place" and that this further required allowing "our graduates of our military and intelligence units to merge into companies with local partners and foreign partners."

The direct tie-ins of SUNC to Israel's government and the successful effort led by SUNC

The direct tie-ins of SUNC to Israel's government and the successful effort led by SUNC and other companies and organizations to place former military intelligence and intelligence operatives in strategic positions in major multinational technology companies reveal that this "deliberate policy" has had a major and undeniable impact on the global tech industry, especially in Silicon Valley.

# Mossad gets its own In-Q-Tel

This "deliberate policy" of Netanyahu's also recently resulted in the creation of a Mossad-run venture capital fund that is specifically focused on financing Israeli tech start-ups. The venture capital fund, called Libertad, was first announced by Israel's Prime Minister's Office and was created with the explicit purpose of "increasing the Israeli intelligence agency's knowledge base and fostering collaboration with Israel's vibrant startup scene" It was modeled after the CIA's venture capital fund In-Q-Tel, which invested in several Silicon Valley companies turned government and intelligence contractors — including Google and Palantir — with a similar goal in mind.

Libertad declines to reveal the recipients of its funding, but announced last December that it had chosen five companies in the fields of robotics, energy, encryption, web intelligence, and natural language processing and text analysis. In regard to its interest in web intelligence, a Mossad employee told *the Jerusalem Post* that the intelligence agency was specifically interested in "innovative technologies for **[the] automatic identification of personality characteristics – personality profiling – based on online behavior and activity**, using methods based on statistics, machine learning, and other areas." (emphasis added)

According to Libertad's website, in return for its investment, now set at NIS 2 million (~$580,000) per year per company, "the Mossad will receive access to the IP [initial product] developed during R&D [Research and Development] while under contract, and a non-commercial, non-exclusive license to use it. Libertad's contract with the company will not provide it with any additional rights." In an interview with *Calcalist Tech*, Mossad Director Yossi Cohen told the paper that the Mossad's partnership with civilian companies in Israel is "excellent" and that the agency will continue to strengthen those ties.

Israeli intelligence has a documented history in placing "backdoors" into technology products for the purpose of surveillance, with one well-known case being Israel's

repurposing of the PROMIS software, discussed in Part III of *MintPress'* series on Jeffrey Epstein. Furthermore, given that U.S. intelligence, specifically the NSA, had "backdoors" placed into the products of major Silicon Valley companies (a service performed by Israeli intelligence-linked tech companies no less), Mossad may very well plan on doing the same with the technology products of companies it backs through Libertad.

Tim Shorrock, investigative journalist and author of *Spies For Hire: The Secret World of Intelligence Outsourcing*, told *MintPress* that the Mossad's continuation of such practices through Libertad was definitely plausible, especially given what Shorrock described as the "unusual" choice of Libertad choosing not to release the identities of the companies in which it invests.

"The Mossad is trying to hide what they are investing in," Shorrock stated, adding that Libertad's secrecy "raises a lot of questions" particularly given that it was modeled after the CIA's In-Q-Tel. Shorrock noted that In-Q-Tel and other venture capital funds with ties to U.S. intelligence or the U.S. military rarely, if ever, hide the identities of the companies they finance.

However, Libertad is merely the latest and most public expression of the Mossad's interest in Israeli tech start-ups, the lion's share of which are created by veterans of Unit 8200 or other Israeli intelligence agencies. Indeed, former Mossad Director Tamir Pardo stated in 2017 that "everyone" in the Israeli cybertechnology sector is an "alumni" of either Israeli intelligence, like the Mossad, or Israeli military intelligence, like Unit 8200. Pardo even went as far as to say that the Mossad itself is "like a start-up."

Pardo himself, after leaving his post as Mossad director in 2016, dove straight into the world of Israeli tech start-ups, becoming chairman of Sepio Systems, whose two CEOs are former Unit 8200 officers. Sepio Systems' advisory boardincludes the former chief information security officer of the CIA, Robert Bigman; former member of the U.S. Military's Joint Special Operations Command (JSOC), Geoff Hancock; and former head of the Israel National Cyber Bureau and veteran of Israeli military intelligence, Rami Efrati. Sepio Systems' cybersecurity software has been adopted by several banks, telecom and insurance companies, including in the U.S. and Brazil.

Pardo is not the only prominent figure in Israel's intelligence community to compare Israeli intelligence agencies to tech start-ups. Shin Bet Director Nadav Argaman described Israel's domestic spy agency in similar terms. "The Shin Bet is like an evolving start-up, with unmatched strength," Argaman stated in a June 2017 speech, as he extolled the agency's use of "pre-crime" technology to detain Palestinians based on their social media

agency's use of "pre-crime" technology to detain Palestinians based on their social media activity.

Argaman, at the time, claimed that more than 2,000 Palestinians, whom he described as "potential lone-wolf terrorists," had been arrested as a result of these "breakthrough technological advances" that use artificial-intelligence algorithms to monitor the social media accounts of Palestinians, especially younger Palestinians, for the use of "tripwire" phrases that have been used by Palestinians who later committed acts of violence. In the case of those who use such terms, "their phones are tracked to see if they meet other suspects, or leave their districts to move towards potential Israeli targets. In such cases, security forces detain the suspect," according to a 2017 report on the practice by *The Economist*.

# The road to fascism, paved by a corrupted PROMIS

Though Israeli intelligence's interest in tech companies goes back several years, there is a well-documented history of Israeli intelligence using bugged software to surveil and gain "backdoor" access to government databases around the world, particularly in the United States.

As was mentioned in Part III of *MintPress'* Epstein series, a sinister yet cunning plan was executed to place a backdoor for Israeli intelligence into the Prosecutor's Management Information System (PROMIS) software, which was then being used by the U.S. Department of Justice and was the envy of government agencies, particularly intelligence agencies, around the world. This bugged version of PROMIS — born out of the collusion between Earl Brian, Ronald Reagan's then-envoy to Iran, and Rafi Eitan, then-director of the now-defunct Israeli intelligence agency Lekem — was seeded around the world by Brian's company Hadron as well as by Mossad-linked media mogul Robert Maxwell, father of Jeffrey Epstein's long-time girlfriend and alleged madam, Ghislaine Maxwell.

After this first PROMIS "backdoor" was discovered, Israel would again gain access to sensitive U.S. government communications, as well as civilian communications, thanks to the collusion between Israeli intelligence and Israeli telecom and tech companies, especially Amdocs and Comverse Infosys (now Verint), that were operating throughout the United States. Today, Unit 8200-linked start-ups appear to have taken up

throughout the United States. Today, Unit 8200-linked start-ups appear to have taken up the torch.

While the PROMIS software is perhaps best known for offering Israeli intelligence a backdoor into as many as 80 intelligence agencies and other sensitive locations around the world for nearly a decade, it was also used for a very different purpose by prominent officials linked to Iran-Contra.

One key Iran-Contra figure — Lt. Col. Oliver North, then serving on the National Security Council — decided to use PROMIS neither for espionage nor for foreign policy. Instead, North turned PROMIS' power against Americans, particularly perceived dissidents, a fact that remained unknown for years.

Beginning in 1982, as part of the highly classified Continuity of Government (COG) program, North used the PROMIS software at a 6,100-square-foot "command center" in the Department of Justice, as well as at a smaller operations room at the White House, to compile a list of American dissidents and "potential troublemakers" if the COG protocol was ever invoked.

According to a senior government official with a high-ranking security clearance and service in five presidential administrations who spoke to *Radar* in 2008, this was:

> **"A database of Americans, who, often for the slightest and most trivial reason, are considered unfriendly, and who, in a time of panic might be incarcerated. The database can identify and locate perceived 'enemies of the state' almost instantaneously."**

In 1993, Wired described North's use of PROMIS in compiling this database as follows:

> **"Using PROMIS, sources point out, North could have drawn up lists of anyone ever arrested for a political protest, for example**

**lists of anyone ever arrested for a political protest, for example, or anyone who had ever refused to pay their taxes. Compared to PROMIS, Richard Nixon's enemies list or Sen. Joe McCarthy's blacklist look downright crude."**

The COG program defined this "time of panic" as "a national crisis, such as nuclear war, violent and widespread **internal dissent**, or **national opposition to a US military invasion abroad,**" whereby the government would suspend the Constitution, declare martial law, and incarcerate perceived dissidents and other "unfriendlies" in order to prevent the government's (or then-serving administration's) overthrow.

This secretive database has often been referred to as "Main Core" by government insiders and, most troubling of all, *it still exists today*. Journalist Christ Ketcham, citing senior government officials, reported in 2008 that, at that time, Main Core was believed to contain the names of as many as 8 million Americans. Eleven years later, it is highly likely that the number of Americans included in the Main Core database has grown considerably.

Author and investigative journalist Tim Shorrock also covered other disturbing aspects of the evolution of Main Core back in 2008 for *Salon*. At the time, Shorrock reported that the George W. Bush administration was believed to have used Main Core to guide its domestic surveillance activities following the September 11 attacks.

Citing "several former U.S. government officials with extensive knowledge of intelligence operations," Shorrock further noted that Main Core — as it was 11 years ago at the time his report was published — was said to contain "a vast amount of personal data on Americans, including NSA intercepts of bank and credit card transactions and the results of surveillance efforts by the FBI, the CIA and other agencies."

Bill Hamilton, former NSA intelligence officer and the original creator of the PROMIS software, told Shorrock at the time that he believed that "U.S. intelligence uses PROMIS as the primary software for searching the Main Core database" and had been told as much by an intelligence official in 1992 and an NSA official in 1995. Dan Murphy, former deputy director at the CIA, had told Hamilton that the NSA's use of PROMIS was "so seriously wrong that money alone cannot cure the problem." "I believe in retrospect that Murphy was alluding to Main Core," Hamilton had told Shorrock.

Though most reporting on Main Core, from the time its existence was first revealed to the present, has treated the database as something used by the U.S. government and U.S. intelligence for domestic purposes, *MintPress* has learned that Israeli intelligence was also involved with the creation of the Main Core database. According to a former U.S. intelligence official with direct knowledge of the U.S. intelligence community's use of PROMIS and Main Core from the 1980s to 2000s, Israeli intelligence played a role in the U.S. government's deployment of PROMIS as the software used for the Main Core domestic surveillance database system.

Israeli intelligence remained involved with Main Core at the time of the August 1991 death of journalist Danny Casolaro, who was investigating not only the government's misuse of the stolen PROMIS software but also the Main Core database. This same official, who chose to remain anonymous, told *MintPress*that, shortly before his death, Casolaro had obtained copies of computer printouts from the PROMIS-based Main Core domestic surveillance database system from NSA whistleblower Alan Standorf, who was found murdered a few months before Casolaro's lifeless body would be found in a West Virginia hotel room.

The source also stated that Main Core's contents had been used for the political blackmail of members of Congress and their staff, journalists, and others by Walter Raymond, a senior CIA covert operator in psyops and disinformation who served on President Reagan's National Security Council during and after Main Core's creation. If used for this purpose by Raymond in the 1980s, Main Core has also likely been used by other individuals with access to the database for blackmailing purposes in the years since.

Given that Israeli intelligence was known to have placed a backdoor into the PROMIS software, before it was marketed and sold around the world by Earl Brian and Robert Maxwell, its role in the U.S. government's decision to use PROMIS in the creation of Main Core suggests that Israeli intelligence likely advocated for the version of PROMIS containing this backdoor, thereby giving Israeli intelligence access to Main Core. Given that Reagan aides and officials colluded with Israeli "spymaster" Rafi Eitan in his efforts to create a backdoor into the software for Israeli military intelligence, the use of this version of PROMIS in the Main Core database is certainly plausible.

Furthermore, the fact that Israeli intelligence was known to be involved in Main Core nearly a decade after its creation suggests that Israeli intelligence may have played a role in certain aspects of the database, such as the criteria used to flag Americans as "unfriendly," and — like Walter Raymond — may have used information in the database to

"unfriendly," and — like Walter Raymond — may have used information in the database to blackmail Americans. In addition, the fact that the cooperation between U.S. and Israeli intelligence, particularly between Unit 8200 and the NSA, has only grown since 1991 further suggests that Israeli involvement in Main Core continues to the present.

While Main Core's very existence is troubling for many reasons, the alleged involvement of a *foreign* intelligence service in the creation, expansion and maintenance of a database with personal details and potentially damaging information on millions of Americans targeted for detention or increased surveillance in times of crisis is chilling. It is especially so considering that the Trump administration's latest proposals to prevent mass shootings before they occur are likely to use Main Core to flag certain Americans for increased surveillance or potentially detention, as was done by the George W. Bush administration following the September 11 attacks.

It appears that Main Core serves a dual purpose; first as a mass targeted surveillance system to crush dissent during times of "national crisis" — whether spontaneous or engineered — and, second, as a massive blackmail database used to keep every potential opponent in line during non-emergencies.

# Peter Thiel's Seeing Stone

As was mentioned earlier in this report, Palantir — the company co-founded by Peter Thiel — is set to profit handsomely from the Trump administration's plans to use its "pre-crime" technology, which is already used by police departments throughout the country and also used to track Americans based on the company's integrative data-mining approach. Palantir, named for the "seeing stones" in the *Lord of the Rings* novels, also markets software to foreign (and domestic) intelligence agencies that predicts the likelihood that an individual will commit an act of terrorism or violence.

Aside from its "pre-crime" products, Palantir has come under fire in recent years as a result of the company's contracts with Immigration and Customs Enforcement (ICE), where it created an intelligence system known as Investigative Case Management (ICM). *The IB Times* described ICM as "a vast 'ecosystem' of data to help immigration officials in identifying targets and creating cases against them" and also "provides ICE agents with access to databases managed by other federal agencies." ICM further gives ICE access to "targets' personal and sensitive information, such as background on schooling, employment, family relationships, phone records, immigration history

schooling, employment, family relationships, phone records, immigration history, biometrics data, criminal records as well as home and work addresses." In other words, Palantir's ICM is essentially a "Main Core" for immigrants.

Notably, part of Oliver North's original intentions in "Main Core" was to trackimmigrants then coming from Central America as well as Americans who opposed Reagan era policy with respect to Central America. At that time, Main Core was believed to be controlled by the Federal Emergency Management Administration (FEMA), which is now part of the Department of Homeland Security (DHS).

*VICE News* reported in July that the Northern California Regional Intelligence Center, which is run by DHS, "serves around 300 communities in northern California and is what is known as a 'fusion center,' a Department of Homeland Security intelligence center that aggregates and investigates information from state, local, and federal agencies, as well as some private entities, into large databases that can be searched using software like Palantir. " *VICE* further noted that this center alone used Palantir to surveil as many as 8 million Ameicans. There are many more such DHS "fusion centers" throughout the United States.

If the Trump administration moves forward with its proposal of employing technology to detect potential mass shooters before they strike, Palantir's technology is set to be used, given that it has already been used by U.S. law enforcement and U.S. intelligence to determine which people run "the highest risk of being involved in gun violence," according to an investigation of Palantirby *The Verge*. Furthermore, Palantir's close ties to the Trump administration make the company's role in a future nationwide "pre-crime" prevention system based on technology appear inevitable.

Palantir founder Peter Thiel listens to Trump during a meeting at Trump Tower in New York, Dec. 14, 2016. Evan Vucci | AP

Worse still is the apparent overlap between Palantir and Main Core. Palantir — which has obvious similarities to PROMIS — is already known to use its software to track potential terror threats, including domestic terror threats, and a category of people it refers to as "subversives." Palantir's tracking of these individuals "is all done using prediction." Palantir's close ties to the U.S. intelligence community suggest that Palantir may already have access to the Main Core database. Tim Shorrock told *MintPress* that Palantir's use of Main Core is "certainly possible," particularly in light of the company's use of the term "subversive" to describe a category of people that its software tracks.

Palantir also has alleged ties to Israeli intelligence, as there have long been suspicions that Israeli intelligence has used Palantir as part of its AI "pre-crime" algorithms targeting Palestinians after Palantir opened a research and development (R&D) center in Israel in 2013. The current head of Palantir Israel, Hamultal Meridor, previously founded a brain-machine interface organization and was senior director of web intelligence at Verint (formerly Comverse Infosys), which has deep connections to Unit 8200, a history of espionage in the United States and was one of the two companies contracted by the NSA to insert a "backdoor" into the U.S. telecommunications system and popular products of major American tech companies.

Given the above, Peter Thiel's 2018 decision to fund Carbyne, the Unit 8200-linked start-up that markets itself as a technological solution to mass shootings in the U.S., strongly suggests that Thiel has been anticipating for some time the now-public efforts of the Trump administration to employ "pre-crime" technology to track and target Americans who show signs of "mental illness" and "violent tendencies."

# A nightmare even Orwell could not have predicted

In early August, in the wake of the shooting at an El Paso Walmart, President Trump called on big tech companies to collaborate with the Justice Department in the creation of

on big tech companies to collaborate with the Justice Department in the creation of software that "stops mass murders before they start" by detecting potential mass shooters before they cnm act. Though Trump's ideas were short on specifics, there is now a new proposal that would create a new government agency that will use data gathered from civilian electronic devices to identify "neurobehavioral" warning signs, thereby flagging "potential shooters" for increased surveillance and potentially detention.

This new agency, as proposed by the foundation led by former NBC Universal president and vice chairman of General Electric Robert Wright, would be known as the Health Advanced Research Projects Agency (HARPA) and would be modeled after the Defense Advanced Research Projects Agency (DARPA). Per the proposal, recently detailed by the *Washington Post*, the flagship program of HARPA would be "Safe Home" (Stopping Aberrant Fatal Events by Helping Overcome Mental Extremes), which would use "breakthrough technologies with high specificity and sensitivity for early diagnosis of neuropsychiatric violence," specifically "advanced analytical tools based on artificial intelligence and machine learning."

The program would cost an estimated $60 million over four years and would use data from "Apple Watches, Fitbits, Amazon Echo and Google Home" and other consumer electronic devices, as well as information provided by health-care providers to identify who may be a threat.

*The Washington Post* reported that President Trump has reacted "very positively" to the proposal and that he was "sold on the concept." *The Post* also noted that Wright sees the president's daughter, Ivanka, as "the most effective champion of the proposal and has previously briefed her on HARPA himself." Ivanka has previously been cited as a driving force behind some of her father's policy decisions, including his decision to bomb Syria after an alleged chemical weapons attack in 2017.

Liz Fed — president of the Susan Wright Foundation, which is led by Robert Wright and created the proposal for HARPA and "Safe Home" — told *The Post* that the proposal emulated DARPA because "DARPA is a brilliant model that works. They have developed the most transformational capabilities in the world for national security...We're not leveraging the tools and technologies available to us to improve and save lives." Fed further asserted that DARPA's technological approach had yet to be applied to the field of healthcare.

For anyone familiar with DARPA, such claims should immediately sound loud alarm bells, especially since DARPA is already developing its own solution to "mental health" issues in

especially since DARPA is already developing its own solution to "mental health" issues in the form of a "brain-machine interface" as part of its N3 program. That program, according to reports, involves "noninvasive and 'minutely' invasive neural interfaces to both read and write into the brain," help distance soldiers "from the emotional guilt of warfare" by "clouding their perception" and "to program artificial memories of fear, desire, and experiences directly into the brain." Though N3 is intended to improve the prowess of American soldiers, it is also set to be used as a means of pursuing DARPA's Systems-Based Neurotechnology for Emerging Therapies (SUBNETS) project, which aims to "to develop a tiny, implanted chip in the skull to treat psychiatric disorders such as anxiety, PTSD and major depression."

Given that HARPA's lead scientific adviser is Dr. Geoffrey Ling, former director and founder of DARPA's Biological Technologies Office (BTO), which "merges biology, engineering, and computer science to harness the power of natural systems for national security," it seems likely that DARPA's neurological-focused research programs, like SUBNETS and N3, would be folded into HARPA's portfolio, making the proposed agency's approach to mental health very questionable indeed.

Aside from the dystopian nature of both DARPA and potentially HARPA's approach to mental health, there is grave cause for concern regarding the Trump administration's moves to address U.S. mass shooting events by implementing pre-crime technology based on artificial intelligence, data-mining and mass surveillance, technologies already laying in wait thanks to companies like Palantir and numerous Israeli tech start-ups led by former Unit 8200 officers.

With companies like Carbyne — with its ties to both the Trump administration and to Israeli intelligence — and the Mossad-linked Gabriel also marketing themselves as "technological" solutions to mass shootings while also doubling as covert tools for mass data collection and extraction, the end result is a massive surveillance system so complete and so dystopian that even George Orwell himself could not have predicted it.

Following another catastrophic mass shooting or crisis event, aggressive efforts will likely follow to foist these "solutions" on a frightened American public by the very network connected, not only to Jeffrey Epstein, but to a litany of crimes and a frightening history of plans to crush internal dissent and would-be dissenters in the United States.

Feature photo | Graphic by Claudio Cabrera

cia epstein Epstein Series intelligence israel mossad Thiel

Author

**Whitney Webb**

Whitney Webb has been a professional writer, researcher and journalist since 2016. She has written for several websites and, from 2017 to 2020, was a staff writer and senior investigative reporter for Mint Press News. She is contributing editor of Unlimited Hangout and author of the book *One Nation Under Blackmail*.