Why a Shadowy Tech Firm With Ties to Israeli Intelligence Is Running Doomsday Election Simulations

A shadowy tech firm with deep ties to Israeli intelligence and newly inked contracts to protect Pentagon computers is partnering with Lockheed Martin to gain unprecedented access to the heart of America's democracy.

BY **WHITNEY WEBB** JANUARY 4, 2020 23 MINUTE READ

This article was originally published on MintPress News

Election Day 2020: 32 Americans dead, over 200 injured, martial law declared and the election itself is canceled. While this horrific scenario seems more like the plot of a Hollywood film, such was the end result of a recent simulation examining the preparedness of U.S. officials from the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS) and the U.S. Secret Service against "bad actors" seeking to undermine the upcoming presidential election.

Yet, this simulation was not a government-organized exercise but was instead orchestrated by a private company with deep ties to foreign and domestic intelligence services, a company that is also funded by investors with clear connections to individuals who would stand to benefit if such a catastrophic election outcome were to become reality.

Much of the rhetoric since the last presidential election in 2016 has focused on the issue of foreign meddling by U.S. rival states like Russia, while China has emerged as the new "meddler" of choice in American corporate media as the 2020 election approaches. Though time has revealed that many of the post-2016 election meddling claims were not as significant as initially claimed, the constant media discussion of foreign threats to U.S. democracy and electoral processes – whether real or imagined – has undeniably created a climate of fear.

Those fears have since been preyed upon by neoconservative groups and the U.S. military-industrial complex, both of which are hardly known for their love of demcratic processes, to offer a series of ready-made solutions to these threats that actually undermine key pillars of American democracy, including independent reporting and voting machine software.

However, many of the very same media outlets and groups that frequently fretted about Russia, China or another rival state meddling in U.S. democracy have largely ignored the role of other nation states, such as Israel, in efforts to sway the last U.S. election in 2016 and meddle in numerous elections in Africa, Latin America and Asia in the years since.

As a consequence of this climate of fear, it should be hardly surprising that the corporate media lauded the recent 2020 election simulation that ended in an abysmal failure for U.S. officials, the cancellation of the U.S. election and the imposition of martial law. Yet, none of those reports on the exercise noted that the company that hosted the simulation, called Cybereason, is led by ex-members of Israel's military intelligence unit 8200, advised by former top and current officials in both Israeli military intelligence and the CIA. In addition, it is funded by and partnered with top U.S. weapons manufacturer and government contractor Lockheed Martin and financial institutions with clear and direct ties to Saudi Crown Prince Mohammed bin Salman and White House adviser and the president's son-in-law Jared Kushner. Also left unmentioned in media reports on Cybereason's election simulations is the fact that Cybereason's CEO, Lior Div, has openly admitted that he views his work at Cybereason as a "continuation" of his service to Israel's intelligence apparatus.

With Cybereason planning to host more simulations in cooperation with federal agencies as the U.S. election inches closer, a deeper exploration of this company, its ties to intelligence and military contractors in the U.S. and Israel and its financial ties to key Trump allies both domestically and abroad warrants further investigation.

In this two part series, *MintPress* will not only explore these aspects but also how many of the technologies wielded by the "bad actors" in the Cybereason election simulation have been pioneered and perfected, not by U.S. rival states, but by Israeli companies and start-ups with clear ties to that country's intelligence apparatus.

Also notable is the fact that Cybereason itself has covertly become a major software provider to the U.S. government and military through its direct partnership with Lockheed Martin, which followed the defense company's decision to open an office at the Israeli military's new cyber operations hub in the Negev desert. In examining all of these interlocking pieces, a picture emerges of a potentially sinister motive for Cybereason's simulations aimed at gauging how U.S. federal officials respond to crisis situations on Election Day.

Understanding “Operation Blackout”

In early November, a team of “hackers” working for the private U.S.-based, Israeli-founded company Cybereason conducted a 2020 election simulationwith members of various U.S. agencies, namely the DHS, FBI and the U.S. Secret Service. The simulation was organized by Cybereason and the law firm Venable and the U.S. agencies in attendance were invited and appear to not have been charged to participate.

The simulation, titled “Operation Blackout,” was set in a fictional swing state called “Adversaria” and pitted “ethical hackers” from Cybereason against a team of federal and local law enforcement officials. The opposing teams were supervised by a “white team” composed of members of Cybereason’s staff and Ari Schwartz — a former member of the White House’s National Security Council and the National Institute of Standards and Technology (NIST) — who set the rules of the simulation and would ultimately decide its outcome. Schwartz also used to work for the Center for Democracy and Technology (CDT), a major backer of Microsoft’s ElectionGuard software.

Operation Blackout did not involve hackers targeting election software or voting machines, instead, it focused on civilian infrastructure and psychological operations against the American citizens in the fictitious “Adversaria” on election day. The hacker team was led by Cybereason co-founder Yonathan Striem-Amit, a former contractor for Israeli government agencies and a former operative for the elite Israeli military intelligence Unit 8200, best known for its cyber offensives against other governments.

“In a country as fragmented as the US, the number of people needed to influence an election is surprisingly small,” Striem-Amit told *Quartz* of the exercise. “We attempted to create havoc and show law enforcement that protecting the electoral process is much more than the machine.”

Streim-Amit’s team completely devastated the U.S. law enforcement team in Operation Blackout by not only causing chaos but murdering numerous civilians. Hackers took control of city buses, ramming them into civilians waiting in line at polling stations, killing 32 and injuring over 200. They also took control of city traffic lights in order to cause traffic accidents, used so-called “deepfakes” to conduct psychological operations on the populace and created fake bomb threats posing as the terror group ISIS, which incidentally has its own ties to Israeli intelligence. Telecom networks and news outlets within the fictitious states were also hacked and flooded with deepfakes aimed at spreading disinformation and panic among U.S. citizens.

The supervising team, composed of Cybereason employees and former NSC member Ari Schwartz, decided that the outcome of the face-off between the hacker and law enforcement teams was the outright cancellation of the 2020 election, the declaration of martial law by authorities, the growth of public fear regarding terrorism and allegations of U.S. government collusion with a foreign actor. Cybereason has stated that they will soon conduct another 2020 election simulation with federal authorities as the election draws closer.

Given how the simulation played out, it is quite clear that it is a far cry from the actual scope of alleged foreign meddling during the 2016 election, meddling which was allegedly the motivation behind Operation Blackout. Indeed, the extent of Russian interference in the 2016 election amounted to $100,000 worth of Facebook ads over three years, 25 percent of which were never seen by the public, and claims that Russian state actors were responsible for leaking emails from the then-Democratic presidential

nominee Hillary Clinton and the Democratic National Committee (DNC). In contrast, Operation Blackout went well beyond any observed or even imagined "foreign meddling" related to the 2016 election and appears more like a terror attack targeting elections than a covert means of manipulating their outcomes.

Several mainstream publications have covered Operation Blackout but have failed to note that the company behind them has deep ties to foreign intelligence outfits and governments with a documented history of manipulating elections around the world, including the 2016 U.S. election.

Quartz framed the exercise as important for "preparing for any and all possibilities in 2020," which "has become an urgent task for US regulators and law enforcement." Similarly, *CyberScoop* treated the simulation as a "sophisticated exercise to help secure the vote." Other articles took the same stance.

A series of simulations

In the weeks after the Washington area election simulation, Cybereason repeated the same exercise in London, this time with members of the U.K. Intelligence agency GCHQ, the U.K. Foreign Office and the Metropolitan Police. The law enforcement team in the exercise, which included the U.K. officials, was headed by a Cybereason employee — Alessandro Telami, who formerly workedfor the NATO Communications and Information Agency (NCI). Like the prior simulation conducted in the U.S., Cybereason did not appear to charge U.K. government agencies for their participation in the exercise.

Cybereason has — with little fanfare — been promoting extreme election day scenarios since before the 2016 election. Cybereason's first mention of these tactics appears in a September 2016 blog post written by the company's CEO and former Israeli government contractor Lior Div — a former leader of offensive cyberattacks for the IDF's elite Unit 8200 and a former development group leader at the controversial Israeli-American corporation Amdocs.

Div wrote that hackers may target U.S. elections by "breaking into the computers that operate traffic lighting systems and interfering with the ones around polling stations to create massive traffic jams, "hacking polling companies," and "targeting live election coverage on cable or network television stations." A follow-up post by Div from October 2016 added further meddling tactics such as "cut power to polling stations" and "mess with a voter's mind."div

Two years later, Cybereason held its first election meddling simulation, touting many of these same tactics, in Boston. The simulation focused on local and state responses to such attacks and saw Boston-based Cybereason invite Massachusetts state and local officials as well as Boston police officers and a former police commissioner to participate. "Twitter accounts spreading fake news," "turning off a city's closed-circuit cameras," "hacking self-driving cars and navigation apps," and "targeting a city's 911 call center with a DDoS attack" were all used in the simulation, which saw Cybereason's "ethical hackers" attempt to disrupt election day. Media coverage of the simulation at the time framed it as a necessary preparation for countering "Russian" threats to U.S. democracy. Like the more recent simulations, the mock election was canceled and voter confidence in the electoral process was devastated.

This past July, Cybereason conducted a similar simulation with officials from the FBI, DHS and the Secret Service for the first time. That simulation, which also took place in Boston, was remarkably similar to that which occurred in November. One intelligence officer from DHS who participated in the July exercise called the simulation "very realistic." Another claimed that the simulation was a way of applying "lessons learned from 9/11" by preventing the government's "failure of imagination" that officials have long alleged was the reason for the government's inability to thwart the September 11 attacks. Notably, The U.S. military simulated a scenario in which terrorists flew airplanes into the Pentagon less than a year before the September 11 attacks.

Participating government officials, Cybereason staff and the media have consistently touted the importance of these simulations in securing elections against extreme threats, threats which — to date — have never materialized due to the efforts of foreign or domestic actors on election day. After all, these exercises are only simulations of possibilities and, even if those possibilities seem implausible or unlikely, it is important to be prepared for any eventuality.

But what if the very figures behind these simulations and the investors that fund them had a history of election meddling themselves? Cybereason's deep ties to Israeli intelligence, which has a documented history of aggressive espionage and election meddling in the United States and in several nations worldwide, warrant a deeper look into the firms' possible motives and the myriad conflicts of interest that arise in giving it such unprecedented access to the heart of America's democracy.

What Does Cybereason Do?

Cybereason's interest in terror events during elections seems out of place given that the company itself is focused on selling technological cybersecurity solutions like antivirus and ransomware protection software, software products that would be minimally effective against the type of threat encountered in the company's election day simulations.

Cybereason is often described as offering a comprehensive technological defense platform to companies and governments that combines a next-generation antivirus with endpoint detection and response (EDR), which enables the company to respond to typical viruses and malware as well as sophisticated, complex attacks. The platform makes heavy use of artificial intelligence (AI) and cloud computing and specifically uses Amazon Web Services (AWS), which is used by a litany of private companies as well as U.S. intelligence agencies.

While many cybersecurity platforms combine antivirus and antimalware with EDR and AI, Cybereason claims that their military background is what sets them apart. They have marketed themselves as offering "a combination of military-acquired skills and cloud-powered machine learning to endpoint detection and response" and actively cite the fact that most of their employees are former members of Unit 8200 as proof that they are "applying the military's perspective on cybersecurity to enterprise security."

In 2018, Cybereason's former senior director for intelligence, Ross Rustici, described the platform to *CBR* as follows:

Our founders are ex-Israeli intelligence who worked on the offensive side. They basically wanted to build a tool that would catch themselves. We follow the kill chain model started by Lockheed Martin [now a major investor in Cybereason] and try to interrupt every stage once an intruder's inside a target network."

Lior Div, Cybereason's CEO described the difference between his company's platform and that of past market leaders in this way to *Forbes*:

The old guard of antivirus companies like Symantec and McAfee would install something to block endpoints and you needed to do a lot [of monitoring] to make sure you weren't under attack. We came with a different approach to see the whole enterprise and leverage AI to be able to fully autonomously identify where attackers are and what they're doing."

Thus, in looking at Cybereason's product and its marketing objectively, it seems that the only innovative component of the company's system is the large number of ex-military intelligence officers it employs and its tweaking of a previously developed and automated model for threat engagement, elimination and prevention.

Instead, Cybereason's success seems to owe to its prominent connections to the private and public sectors, especially in Israel, and its investors who have funneled millions into the company's operations, allowing them to expand rapidly and quickly claim a dominant position in emerging technology markets, such as the Internet of Things (IoT) and advanced healthcare systems.

Their considerable funding from the likes of Lockheed Martin and Softbank, among others, has also helped them to expand their international presence from the U.S., Europe and Israel into Asia and Latin America, among other places. Notably, while Cybereason is open about their investors and how much funding they receive from each, they are extremely secretive about their financial performance as a company and decline to disclose their annual revenue, among other indicators. The significance of Cybereason's main investors in the context of the company's election simulations and its ties to Israeli and U.S. intelligence (the focus of this article) will be discussed in Part 2.

Cybereason also includes a security research arm called Nocturnus, currently headed by a former Unit 8200 officer. Nocturnus will be explored further in Part 2 of this series, as it essentially functions as a private intelligence company in the tech sector and has been behind several recent claims that have attributed alleged hacks to state actors, namely China and North Korea. For now, it is important to keep in mind that Nocturnus utilizes Cybereason's "global network of millions of endpoints" for its intelligence gathering and research, meaning the endpoints of every device to which Cybereason's software has access.

Given what Cybereason provides as a company, their interest in offering election simulations to government officials free of charge seems odd. Indeed, in the simulations hosted by Cybereason for U.S. officials, there is little opportunity for the company to market their software products given that the simulation did not involve electronic voting infrastructure at all and, instead, the malevolent actors used deep fakes, disinformation and terror attacks to accomplish their goals. Why then would this company be so interested in gauging the response of U.S. law enforcement to such crises on election day if there is no sales pitch to be made? While some may argue that these simulations are an altruistic effort by the company, an investigation into the company's founders and the company's ties to intelligence agencies suggests that this is unlikely to be the case.

The People Behind Cybereason

Cybereason was created in 2012 by three Israelis, all of whom served together as officers in the Israel Defense Force's elite technological and signals intelligence unit, which is most often referred to as Unit 8200. Unit 8200 has been the subject of several *MintPress* investigative reports over the past yearfocusing on its ties to the tech industry.

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, surveillance, cyberwarfare and code decryption. It is also well-known for its surveillance of Palestinian civilians and for using intercepted communications as blackmail in order to procure informants among Palestinians living under occupation in the West Bank.

The unit is frequently described as the Israeli equivalent of the NSA and Peter Roberts, a 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.

Given the secrecy of the work conducted by Unit 8200, it is hard to know exactly what Cybereason's co-founders did while serving in the controversial unit, however, a brief biography of the company's current CEO and co-founder Lior Div states that "Div served as a commander [in Unit 8200] and carried out some of the **world's largest cyber offensive campaigns against nations** and cybercrime groups. For his achievements, he received the Medal of Honor, the highest honor bestowed upon Unit 8200 members (emphasis added)."

After having served in leadership positions within Unit 8200, all three Cybereason co-founders went on to work for private Israel-based tech or telecom companies with a history of aggressive espionage against the U.S. government.

Cybereason co-founders Yonathan Striem Amit (Cybereason's Chief Technology Officer) and Yossi Naar (Cybereason Chief Visionary Officer) both worked for Gita Technologies shortly before founding Cybereason with fellow Unit 8200 alumnus Lior Div. Gita, according to public records, is a subsidiary of Verint Systems, formerly known as Comverse Infosys.

Verint/Comverse was initially funded by the Israeli government and was founded by Jacob "Kobi" Alexander, a former Israeli intelligence officer who was wanted by the FBI on nearly three dozen charges of fraud, theft, lying, bribery, money laundering and other crimes for over a decade until he was finally extradited to the United States and pled guilty to some of those charges in 2016.

Despite its history of corruption and foreign intelligence connections, Verint/Comverse was hired by the National Security Agency (NSA) to create backdoors into all the major U.S. telecommunications systems and major tech companies, including Facebook, Microsoft and Google. An article on Verint's access to U.S. tech infrastructure in *Wired* noted the following about Verint:

In a rare and candid admission to Forbes, Retired Brig. Gen. Hanan Gefen, a former commander of the highly secret Unit 8200, Israel's NSA, noted his former organization's influence on Comverse, which owns Verint, as well as other Israeli companies that dominate the U.S. eavesdropping and surveillance market. 'Take NICE, Comverse and Check Point for example, three of the largest high-tech companies, which were all directly influenced by 8200 technology,' said Gefen."

Federal agents have reported systemic breaches at the Department of Justice, FBI, DEA, the State Department, and the White House going all the way back to the 1990s, breaches they claimed could all be traced back to two companies: Comverse/Verint and Amdocs. Cybereason's other co-founder and current CEO, Lior Div, used to work for Amdocs as the company's development group leader.

After leaving Amdocs, Div founded a company called Alfatech. Alfatech publicly claims to specialize in "professional Head Hunting and Quality Recruiting services," yet it has no functional website. Despite its publicly stated mission statement, Israeli media reports that mention Alfatech describe it as "a cybersecurity services company for Israeli government agencies." No reason for the obvious disconnect between the company's own claims and those made by the media has been given.

Div left Alfatech in 2012 to found Cybereason alongside Striem-Amit and Naar. According to an interview that Div gave to *TechCrunch* earlier this year, he stated that his work at Cybereason is "**the continuation** of the six years of training and service he spent working with the Israeli army's 8200 Unit (emphasis added)." Div was a high-level commander in Unit 8200 and "carried out some of the world's largest cyber offensive campaigns against nations and cybercrime groups" during his time there.*TechCrunch* noted that "After his time in the military, Div worked for the Israeli government as a private contractor reverse-engineering hacking operations," an apparent reference to his work at Alfatech.

Even deeper ties to intelligence

Not only do Cybereason's own co-founders have considerable links to the Israeli government, Israeli intelligence and intelligence-connected private companies, but it also appears that the work of Cybereason itself is directly involved with Israeli intelligence.

The company periodically publishes reports by a secretive faction of the company called the Cybereason Intelligence Group or CIG. The only descriptionof CIG's composition available on Cybereason's website is as follows:

*The Cybereason Intelligence Group was formed with the unique mission of providing context to the most sophisticated threat actors. The group's members include experts in cyber security and international security **from various government agencies, including the Israel Defense Forces' Unit 8200**, which is dedicated to conducting offensive cyber operations. Their primary purpose is to examine and explain the Who and the Why behind cyber attacks, so that companies and individuals can better protect themselves (emphasis added)."*

It is unclear how many members comprise CIG and if its members are employees of only Israeli government agencies, or if it includes officials from the U.S. government/Intelligence or other

governments. However, what is clear is that it is composed entirely of government officials, which include active members of Unit 8200, and that the purpose of the group is to issue reports that place blame for cyberattacks on state and non-state actors. Perhaps unsurprisingly, the vast majority of CIG's reports published by Cybereason focus exclusively on Russia and China. When discussing nation-state cyber threats in general, Cybereason's website only mentions China, North Korea, Iran and Russia by name, all of which are incidentally rival states of the U.S. government. Notably, Israel's government — listed as a "leading espionage threat" to U.S. financial institutions and federal agencies by the U.S.' NSA — is absent from Cybereason's discussions of state actors.

In addition to CIG, Cybereason's cybersecurity research arm, Nocturnus,includes several Unit 8200 alumni and former Israeli military intelligence and government contractors and has assigned blame to state actors for several recent hacks. It also has claimed to have discovered more such hacks but has declined to publicly disclose them due to the "sensitive" nature of the hacks and companies affected.

Other hints at Cybereason's connections to state intelligence can be seen in its advisory board. Robert Bigman, the former Chief Information Security Officer (CISO) for the Central Intelligence Agency (CIA) who oversaw the spy agency's "commercial partner engagement" program (i.e. alliances with the private tech sector), is a key figure on the company's advisory board. According to his biography, Bigman " contributed to almost every Intelligence Community information security policy/technical standard and has provided numerous briefings to the National Security Council, Congress and presidential commissions. In recognition of his expertise and contributions, Bigman has received numerous CIA and Director of National Intelligence Awards."

Unmentioned in his biography published his own website, or on Cybereason's website, is that Bigman is also an advisor to another Israeli tech company, Sepio Systems. The chairman of Sepio, Tamir Pardo, is a self-described "leader" in the cybersecurity industry and former director of Israel's Mossad. Sepio is funded by a venture capital firm founded by the creators of the controversial Israeli spy tech company NSO Group, which has received a slew of negative press coverage after its software was sold to several governments who used it to spy on dissidents and human rights activists.

In addition to Bigman, Cybereason's advisory board includes Pinchas Buchris, the former head of Unit 8200 and former managing director of the IDF. Not unlike Bigman, Buchris' bio fails to mention that he sits on the board of directors of Carbyne911, alongside former Israeli Prime Minister Ehud Barak and Nicole Junkerman, both well-known associates of intelligence-linked sex trafficker Jeffery Epstein. Epstein himself poured at least $1 million into Carbyne, an Israeli company that seeks to run all 911 call centers in the U.S. at the national level and has close ties to the Trump administration. More information on Carbyne and its ties to Israeli and U.S. intelligence as well as its connection to coming pre-crime policies to be enacted in 2020 by the U.S. Department of Justice can be found in this *MintPress* report from earlier this year. Given that Cybereason's election day simulations involve the simulated collapse of 911 call center functionality, Buchris' ties to both Cybereason and Carbyne911 are notable.

Another notable Cybereason advisor is the former commissioner of the Boston Police Department, Edward Davis. Davis heavily promoted Cybereason's disturbing election day simulations and even participated directly in one of them. He was also police commissioner of the Boston PD at the time of the Boston Marathon bombing and oversaw the near-martial law conditionsimposed on the city during the manhunt for the alleged perpetrators of that bombing (who themselves had a rather odd relationship with the FBI). This is notable given that Cybereason's election day simulations ended with martial law being imposed on the fictional city used in the exercise

Cybereason also has several advisors who hold top positions at powerful U.S. companies that are also — incidentally — U.S. government contractors. These include the Vice President Security and Privacy Engineering at Google, Deputy Chief Information Security Officer (CISO)

of Lockheed Martin and CISO at Motorola. Both Motorola and Lockheed Martin use Cybereason's software and the latter is also a major investor in the company. Furthermore, as will be explained in Part 2 of this article, Lockheed Martin has used its privileged position as the top private contractor to the U.S. government to promote the widespread use of Cybereason's software among U.S. government agencies, including the Pentagon.

Much more than a cybersecurity company

Given Cybereason's deep and enduring ties to Israeli intelligence and its growing connections to the U.S. military and U.S. intelligence through its hiring of top CIA officials and partnership with Lockheed Martin, it's worth asking if these disturbing election simulations could serve an ulterior purpose and, if so, who would benefit. While some aspects regarding clear conflicts of interest in relation to the 2020 election and Cybereason will be discussed in Part 2, this article will conclude by examining the possibility that of Cybereason is acting as a front company for Israeli intelligence based on that country's history of targeting the U.S. through private tech companies and on Cybereason's own questionable characteristics.

First, Cybereason as a company presents several oddities. Its co-founder and CEO openly states that he views Cybereason's work as a continuation of his service for Israeli military intelligence. In addition, he and the company's other founders — after they left Unit 8200 — went to work for Israeli tech companies that have been known to spy on U.S. federal agencies for the Israeli government.

In addition, as previously mentioned, Cybereason has sought out former intelligence officers from the CIA and Unit 8200 for its management team and board of advisors. The company itself also functions as a private intelligence firm through CIG and Nocturnus, both of which employ former and current intelligence officials, and have made significant claims regarding the attribution of specific cybercrimes to state actors. It appears highly likely that these claims are influenced by those same intelligence agencies that boast close ties to Cybereason. Furthermore, Nocturnus' access to Cybereason's "global" network of endpoints makes it a private intelligence gathering company as it gathers and analyzes data from all devices that run Cybereason's software.

Yet, even more telling is the fact that Israel's government has an open policy of outsourcing intelligence-related activity to the private sector, specifically the country's tech sector. As *MintPress* previously reported, this trend was first publicly acknowledged by Israel in 2012, the same year that Cybereason was founded by former Israeli military intelligence officers then-working for private contractors for Israel's government (Alfatech) or private companies known to have ties to Israeli intelligence, including Verint/Comverse.

As noted in an article on the phenomenon from the Israeli media outlet *The Calcalist*:

Israel is siphoning cyber-related activities from its national defense apparatus to privately held companies. 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."

Mention of Israel's policy of blurring the lines between the public and private sector when it comes to cybersecurity and intelligence gathering has even garnered the occasional mention in mainstream media, such as in a 2018 *Foreign Policy* article:

Israel, for one, has chosen to combat the problem on a statewide level by linking the public and private spheres, sometimes literally. The country's cyberhub in the southern city of Beersheba is home not just to the Israeli military's new technology campus but also to a high-tech corporate park, Ben-Gurion University of the Negev's cyber-research center, and the Israel National Cyber Directorate, which reports directly to the prime minister's office. "There's a bridge between them—physically," [Gabriel] Avner, the security consultant, said by way of emphasis."

Notably, a year before Lockheed Martin invested in and partnered with Cybereason, the U.S.-based weapons company opened an office at the IDF's public-private cyber hub in Beersheba. At the inauguration ceremony for Lockheed's Beersheba office, company CEO Marilyn Hewson stated:

The consolidation of IDF Technical Units to new bases in the Negev Desert region is an important transformation of Israel's information technology capability…By locating our new office in the capital of the Negev we are well positioned to work closely with our Israeli partners and stand ready to: accelerate project execution, reduce program risk and share our technical expertise by training and developing in-country talent."

Further evidence of this public-private merger can be seen in how two of Israel's intelligence agencies, Shin Bet and Mossad, have both recently launched a private start-up accelerator and a hi-tech venture capital fund, respectively. The Shin Bet's accelerator, called Xcelerator, usually makes its investments in private companies public, while Mossad's Libertad Ventures refuses to disclose the tech companies and start-ups in which it invests. Former directors of both Mossad and Shin Bet have described these intelligence agencies themselves of being like start-ups, clearly showing how much the line between intelligence apparatus and private company has been blurred within the context of Israel's tech industry and specifically its cybersecurity industry.

The advantages of outsourcing cyber intelligence operations to private companies have been noted by several analysts, including Sasha Romanosky, a former Cyber Policy Advisor at the Department of Defense and current analyst at RAND Corporation. Romanosky noted in 2017 that private intelligence and cybersecurity firms "do not necessarily face the same constraints or potential repercussions" as their public counterparts when it comes to designating blame for a cyberattack, for example. In addition, outsourcing intelligence objectives or missions to private companies provides a government with plausible deniabilityif that private company's espionage-related activities or ties are made public.

Furthermore, Israeli intelligence has a long history of using private tech companies for the purposes of espionage, including against the United States. While Amdocs and Verint/Comverse were already mentioned as having been used by the state of Israel in this way, other private companies have also been used to market software backdoored by Israeli intelligence to countries around the world, both within the U.S. and elsewhere. The most well-known example of this is arguably the mass sale and distribution of the bugged PROMIS software, which was discussed at length in several recent *MintPress News* reports.

Given Cybereason's ties to intelligence and Israeli intelligence's history of placing backdoors in its software, it is worth pointing out that Cybereason's main product, its antivirus and network defense platform, offers a major espionage opportunity. Blake Darché, a former N.S.A. operator, told the *New York Times* in 2017 that antivirus programs, which Cybereason's defense platform includes, is "the ultimate backdoor," adding that it "provides consistent, reliable and remote access that can be used for any purpose, from launching a destructive attack to conducting espionage on thousands or even millions of users." Whether a company like Cybereason would use its software for such ends is unknown, though the company does acknowledge that its cybersecurity arm does gather intelligence from all systems that use the company's software and currently employs and works with active duty Unit 8200 officials through CIG. This is notable because Unit 8200's main task for Israeli military intelligence is signals intelligence, i.e. surveillance.

More of a mystery, however, is why a company like Cybereason is so interested in U.S. election security, particularly when Israeli intelligence and Israeli intelligence-connected private companies have been caught in recent years meddling in elections around the world, including the United States.

cybersecurity intelligence israel simulations tech u.s. elections

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 currently writes for The Last American Vagabond.

11 comments

Mick says:
August 2, 2020 at 12:59 am

Every time I consider the next Israeli 'false flag' operation I can't help but recall this conversation from the London 7/7 operation.

Listen from the save point…

https://www.youtube.com/watch?v=aGE9FiuM06o
Reply

Bleez says:
August 2, 2020 at 1:03 am

Excellent, thanks Whitney. Look forward to the next pieces in the series.
Reply

Blinky The Doormat says:
August 2, 2020 at 6:26 am

I think people are afraid to comment less a Danny Casolaro like event befalls them. But then that just might be my imagination running away from me …
Reply

Timothy R Sammet says:
October 23, 2020 at 5:04 am

Thank you for your time spent researching and writing, it's a very informative article and much appreciated!
Reply

Devyn says:
December 2, 2020 at 11:05 pm

SOS I'm stuck in a simulation in Kalmazoo Michigan
Reply

สมัคร gclub ไม่มีขั้นต่ำ says:
March 17, 2021 at 5:48 pm

Think positively and have fun. Work hard and **สมัคร** gclub **ไม่มีขั้นต่ำ** don't give up hope. Be open to constant criticism and learning. Surround yourself with happy, warm and friendly people.
Reply

เว็บพนันออนไลน์ ไม่ผ่านเอเย่นต์ says:
March 18, 2021 at 2:00 pm

One trend is part efforts to fully assist online **เว็บพนันออนไลน์ ไม่ผ่านเอเย่นต์** football gambling options in the form of the holidays. To assign an opportunity to build on the part that will plan to eat long-term profits in the future
Reply

เว็บพนันออนไลน์ ไม่ผ่านเอเย่นต์ says:
March 18, 2021 at 2:05 pm

One trend is part efforts to fully assist online **เว็บพนันออนไลน์ ไม่ผ่านเอเย่นต์** football gambling options in the form of the holidays. To assign an opportunity to build on the part that will plan to eat long-term profits in the future
Reply

เกมสล็อต gclub says:
April 2, 2021 at 2:31 pm

It was a very nice post and **เกมสล็อต** gclub also informative, thanks for sharing this amazing post.
Reply