How Government And Media Are Prepping America For A Failed 2020 Election

Description

Authored by Whitney Webb via MintPressNews.com,

Best Known Deep Fake Creator is Funded by Israeli Intelligence

While the media, and even Cybereason itself, have helped lay the foundation to blame specific state actors for 2020 election meddling well ahead of the fact, it is worth revisiting Cybereason's "Operation Blackout" election simulation and the tactics used by the "bad actors" in that scenario.

That simulation, discussed in detail in the first installment of this series, saw the weaponization of specific technologies, namely deep fakes, hacks of Internet of Things (IoT) devices and hacks of vehicles, in order to target the 2020 U.S. election, resulting in the cancellation of the election and the imposition of martial law.

Given the current narrative regarding what state actors are likely to meddle in the 2020 election — namely Russia, China and Iran — and the tactics they will allegedly use, it is important to explore the sources of the technologies weaponized per that narrative as well as in "Operation Blackout."

Indeed, if there is any clear overlap between the creators of those technologies and the state actors being blamed in advance for their imminent use, it would certainly lend credibility to the claims promoted by U.S. intelligence, the media and companies like Microsoft and Cybereason.

Yet, upon closer examination, it becomes clear that the companies and state actors most involved in developing these technologies are the very ones claiming that Russia, China and Iran will use them to undermine the 2020 election.

Take for instance the use of deep fakes. Not only have numerous media reports focused on how deep fakes will be used to meddle in the 2020 elections, but Cybereason's doomsday election simulation saw "bad actors" rely heavily on their use to spread disinformation and even make fake bomb threats. While much has been said of the coming election and deep fakes, remarkably few reports have bothered to look at the company best known for creating viral deep fakes.

Canny AI has garnered considerable media attention over the past few years for its persuasive deep fake videos that have frequently gone viral. In the last year alone, the tech firm's viral deep fakes have included a controversial video of Mark Zuckerberg where the Facebook co-founder appears to be saying "Imagine this for a second: One man, with total control of billions of people's stolen data, alltheir secrets, their lives, their futures," as well as a video showing Richard Nixon giving a speech henever actually gave. **More recently, Canny AI was behind the viral videos immediately prior to the 2019 U.K. general election that appeared to show Jeremy Corbyn and his rival Boris Johnson endorsing each other and another video that showed world leaders singing John Lennon's "Imagine":**

Oddly, many of the media reports that discuss these viral videos fail to mention the role of Canny AI in creating these viral deep fakes and instead only mention the organization or artists with whom Canny AI partnered to create them. For instance, the Corbyn-Johnson videos were reported to have been produced by the group Future Advocacy and artist Bill Posters, but it was actually Canny AI that created those videos for that group. Similarly, the Nixon Speech deep fake was reported by several outlets as having been solely created by MIT's Center for Advanced Virtuality. However, the Boston Globe noted that "the [MIT] team worked with Canny AI, an Israeli company that does Video Dialogue Replacement, and Respeecher, a Ukrainian startup specializing in speech-to-speech synthetic voice production" to create the video.

The Zuckerberg deep fake that Canny AI created led to lots of positive press for the company, with several media reports dubbing them as the company using "deep fakes for good" and that uses the controversial technology "responsibly." The Zuckerberg deep fake has been cited as one of the main drivers behind Facebook's new "deep fake" policy, which only bans some deep fake videos and has been criticized by U.S. lawmakers as insufficient. Notably, neither Facebook nor Facebook-owned Instagram ever took down Canny AI's deep fake of Zuckerburg.

Given the concern over deep fakes in relation to the coming election and Canny AI standing out as the main producer of deep fakes that have gone viral over the past year, it is important to point out that Canny AI has ties to a state actor with a history of election meddling: the state of Israel.

Indeed, Canny AI is 100 percent funded by an Israeli start-up accelerator called Xcelerator, a joint venture between Tel Aviv University and Israeli intelligence agency Shin Bet (sometimes called Shabak). According to Start Up Nation Central, the Paul Singer-created organization that promotes Israeli technology start ups, Xcelerator-funded "start-ups participating in the program benefit from **close mentoring from content and technology experts from the Shabak**, experts from Tel Aviv University, and industry leaders. **The connection to the Shabak also provides the entrepreneurs with ways to test the capabilities of their technologies** and cooperation opportunities (emphasis added)."

In addition, Xcelerator is partnered not only with Israeli intelligence directly, but also with Cybereason, the very company that explored the use of deep fakes in the 2020 U.S. presidential election that saw the election cancelled and martial law declared as well as a company that itself has deep ties to Israeli intelligence. Other notable partners of Xcelerator include NEC Corp, which has intimate ties to top Cybereason investor Softbank; Check Point Technologies, which has ties to Israeli military intelligence Unit 8200; and the Israeli start-up accelerator Team8. In previous reports published by MintPress, Team8 was discussed in detail, particularly their recent hire of former director of the NSA

and former head of U.S. Cyber Command Mike Rogers, and their close ties to Paul Singer's Start Up Nation Central, which itself has deep ties to U.S. neoconservatives.

It is also worth noting that Xcelerator also backs an "anti-fake news" start-up called Cyabra, which has direct ties to Israel's Mossad and offers its AI-driven "disinformation protection" to government agencies as well as politicians, particularly during election seasons. Two of Cyabra's co-founders previously co-founded Psy-Group, which attempted to interfere in the 2016 U.S. election by weaponizing "fake news" and social media and later closed down its operations after U.S. government scrutiny into its activities began as part of the Mueller investigation.

Psy-Group also engaged in doxxing campaigns targeting Palesintian rights activists in the U.S. which were planned in conjunction with Ram Ben-Barak, the former deputy director of the Mossad who now advises Cyabra. Given that much of the concern ahead of the next election is related not only to deep fakes but also "fake news," Cyabra's rise and its clear ties to Mossad and the now defunct Psy-Group are important to note.

Furthermore, in examining the other technologies weaponized during Cybereason's 2020 election simulation and cited in the aforementioned media narrative regarding 2020 meddling, a pattern similar to that of Canny AI emerges.

Indeed, the other technologies linked to these "bad actors" and foreign meddlers — namely hacking IoT devices and hacking vehicles — are also pioneered by companies with deep ties to Israeli military intelligence, specifically Unit 8200, and Israeli tech companies that have aggressively spied on U.S. government institutions in collusion with Israeli intelligence in the past, namely Comverse (now Verint) and Amdocs.

Hacking the Internet of Things

In Cybereason's doomsday election simulation, another of the tactics used was the hacking of devices and appliances connected to the internet, often referred to as the Internet of Things (IoT) and which includes everything from smartphones to power grid infrastructure to city traffic lights.

While most reports on IoT hacks to date have focused on "lone wolf" or non-state-aligned actors, one company has stood out for its efforts to create a tool that would allow governments and intelligence agencies to hack these devices with ease. That company, called Toka, announced in 2018 that it planned to offer "a one-stop hacking shop for governments that require extra capability to fight terrorists and other threats to national security in the digital domain," with "a special focus on [hacking] the so-called Internet of Things (IoT), covering tech like Amazon Echo, Nest connected home products, as well as connected fridges, thermostats and alarms."

The Israel-based company, which raised $12.5 million within months of launching, has since been busy marketing its services to governments around the world, most recently France where it described its product portfolio as "empower[ing] governments, Intelligence, and law enforcement agencies to enhance Homeland Security with groundbreaking cyber-intelligence and operational capabilities" during an exposition in Paris last November.

Even though Toka openly markets the ability to hack private consumer devices to governments and law enforcement agencies around the world, the clear threat to privacy has gone ignored by media outlets as the company has garnered nearly no media attention since it launched

nearly two years ago.

Yet, Toka is not only notable for what it offers but also for its founders and investors. Indeed, the co-founders of Toka have been described as an “all-star” team, largely because of the role of former Israeli Prime Minister and former head of Israeli military intelligence, Ehud Barak. Barak, in addition to co-founding the company, serves as its director and is also the chairman of the board of the controversial Israeli company Carbyne911, which markets software to emergency call centers in the United States. Interestingly, Cybereason’s 2020 doomsday election simulation also dealt with the hacking and weaponization of 911 call centers. Also of note is the fact that another of Carbyne911’s leadership team, former Unit 8200 commander Pinchas Buchris, is an adviser to Cybereason.

Toka’s top brass is a who’s who of former Israeli military and intelligence officials

In addition to Barak, **Toka was co-founded by retired Brigadier General Yaron Rosen, former Chief of the IDF’s cyber staff, where he was “the lead architect of all [IDF] cyber activities” including those executed by Israeli military intelligence Unit 8200.** Rosen, who now serves as Toka’s CEO, has stated that Toka’s technology will only be sold to countries allied with the U.S. and Israel, telling Forbes that “Russia, China and ‘other enemy countries’ would never be customers.”

Toka’s leadership and software architects are similarly tied into Israel’s national security state. Several — including the “architect” of its hacking software — previously worked for Israel’s Prime Minister’s Office and developed “offensive technologies” for Israel’s head of state and other top Toka employees and executives share numerous connections to Unit 8200, other divisions of Israeli military intelligence and Unit 8200-connected tech companies like Check Point Technologies.

Though Toka’s leadership team makes its ties to Israeli military intelligence abundantly clear, important connections also appear in examining Toka’s investors. One of the major investors in Toka is Dell technologies, one of the world’s largest technology companies that was founded by Michael Dell, a well-known pro-Israel partisan who has donated millions of dollars to the Friends of the IDF and one of the top supporters of the so-called “anti-BDS” bills that prevent publicly employed individuals or public institutions from supporting non-violent boycotts of Israel, even on humanitarian grounds. It goes

without saying that a major technology company investing in a company that markets the hacking of that very technology (computers, IoT, smartphones, etc.) should be a red flag.

With a major foot in the door through its connections to Dell, whose products are used by the private and public sectors around the world, other investors in Toka again reveal its ties to Israel's military intelligence and the same controversial Israeli tech companies that have aggressively spied on the U.S. government in the past — Amdocs and Comverse. For instance, Entrèe Capital, a venture capital fund that is one of Toka's main investors, is managed by Aviad Eyal and Ran Achituv. The latter, who manages Entrée's investment in Toka and sits on Toka's board of directors, is the founder of the IDF's satellite-based signals intelligence unit and also a former senior Vice President at both Amdocs and Comverse Infosys (Verint).

Another notable investor in Toka is the venture capital firm Andreesen Horowitz, which is advised by former Secretary of the Treasury Larry Summers, a close friend of the infamous pedophile Jeffery Epstein, whose own ties to Israeli military intelligence have been discussed in several MintPress reports. Epstein was also a close friend of Ehud Barak, co-founder and director of Toka, and invested at least $1 million in another company with close ties to Barak, Carbyne911. The remaining investors in Toka are Launch Capital, which is deeply tied to the Pritzker family — one of the wealthiest families in the U.S. with close ties to the Clintons and Obamas as well as the U.S.' pro-Israel lobby, and Ray Rothrock, a venture capitalist who spent nearly three decades at VenRock, the Rockefeller family venture capital fund.

Unit 8200 – From Hacking Cars to Protecting Them?

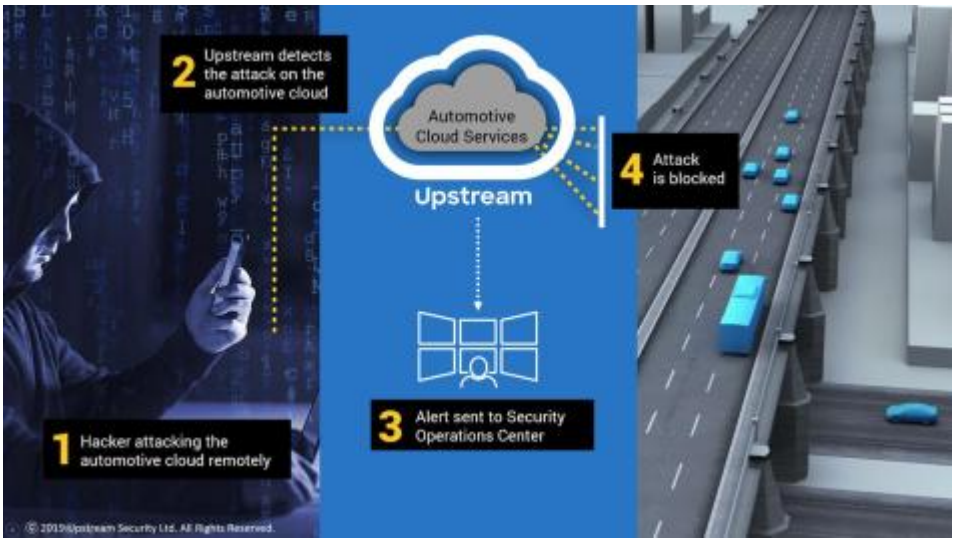
Arguably the most disturbing aspect of Cybereason's "Operation Blackout" election simulation was the hacking of vehicles that were then rammed into civilians waiting in line to vote at polling stations. In the simulation, this led to scores of dead Americans and hundreds of injuries.

As was the case with other technologies used to undermine the 2020 election in the simulation, this technology — the hacking of vehicles — is the bread and butter of an Israeli cybersecurity firm called Upstream Security that specializes in automobiles and boasts deep ties to the country's military intelligence service.

Though vehicle hacking seemed out of left field when the 2020 election simulation took place last November, media reports about the imminent dangers of "car hacking" began to emerge just a month after the exercise took place, most of which cited a December 2019 report created by Upstream. Some of those reports have warned that car hacking could be used to undermine the coming U.S. election.

One report titled "Car Hacking Hits the Streets," cites only Upstream's report to claim that "In 2020, the connected-car market will reach a tipping point, with the majority of vehicles already connected to the Internet when sold in the United States, representing a large base of potential targets for attacks." Another report, titled "New study shows just how bad vehicle hacking has gotten," uses Upstream's report (i.e. study) to claim that hacks of regular vehicles have exploded since 2016 and that most of the cars on U.S. roads today are vulnerable to hackers and that over 80 percent of those hacks occur remotely.

Neither report noted Upstream's ties to Israeli military intelligence. Equally notable is the fact that both reports that covered the Upstream-written study say that only manufacturers can address the problem by partnering with a company like Upstream.



A screenshot from an Upstream promotional video

Lucky for Upstream, they have already partnered with a slew of auto manufacturers, including Hyundai, Volvo, Renault and even U.S. auto insurance giants like Nationwide, who now number among Upstream's most important investors. The company's original investors are Charles River Ventures, one of Cybereason's first investors, and Israeli venture capital firm Glilot Capital.

Glilot Capital's interest in Upstream is telling given the firm's deep ties to Israel's Unit 8200. Glilot was founded by two former Israeli military intelligence officers and has "a heavy focus on the cyber sector and the entrepreneurs who emerge from the elite Unit 8200," according to the Jerusalem Post. Even the name of the firm is an homage to Unit 8200, as the unit's main base is located in Glilot, near Herzliya.

"It's as if Americans called a VC Fort Meade Capital [the US Army base in Maryland where the National Security Agency and the United States Cyber Command are headquartered], some VC names are meant to be symbolic, as in our case. Glilot is the home of several of the best intelligence and technology units in the IDF, it's where we came from and it is where we find our best entrepreneurs," Glilot Capital co-founder Arik Kleinstein told the Jerusalem Post in 2016.

Upstream is certainly the type of company that Glilot Capital is used to investing in. It was founded by two Israelis who both served in the IDF, with one of them serving in an elite intelligence unit. Upstream's co-founders, Yoav Levy and Yonathan Appel, met while working at Check Point Technologies, the Unit 8200 alumni-founded company with deep ties to Israel's military intelligence and military-industrial complex as well as the IoT hacking company Toka. Notably, Upstream recently partnered with the Japanese company Fujitsu, a longtime partner with Softbank — Cybereason's main investor.

Softbank has also invested heavily in another Unit 8200-founded vehicle security start-up called Argus

Cyber Security, a firm known for its numerous demonstrations showing how easy it is to hack vehicles. Argus is also backed by Nadav Zafrir, the former Unit 8200 commander who now runs Team8. Argus' CEO Ofer Ben-Noon, a former captain in Unit 8200, told Forbes in 2014 that "Everything will be hacked in every single [car] brand. It will take time, it might be weeks, months, or a couple of years, but eventually it will happen."

Since then, Unit 8200 alumni from Argus, Upstream and other Israeli automobile cybersecurity firms have shown media outlets around the world how much easier hacking vehicles has become in the years since Ben-Noon first made the claim. One such report from VICE includes a vehicle hacking demonstration, courtesy of a Unit 8200 alumni, and notes that "most cars today are susceptible to hacker attacks."

Of course, Unit 8200 isn't the only intelligence agency known to be experts at hacking vehicles. Indeed, in 2017, WikiLeaks revealed that the CIA was capable of hacking vehicles and exploring their use in committing "undetectable assassinations."

"Bring down nations to their knees"

At the Tel Aviv Cybertech Conference in 2017, Israeli Prime Minister Benjamin Netanyahu stated the following:

> **Today warfare has changed dramatically…With a click of a button, you can bring down nations to their knees very rapidly if you so desire and if you're willing to take the risks, because every system can be hacked. Our hospitals, our airplanes, our cars, our banks. The most important word here is our data banks, they can be hacked."**

Media reports and even members of the Israeli public and private sector have openly acknowledged that Israel's intelligence apparatus — from Unit 8200 to the Mossad — remains directly linked to many of the private technology companies founded by its former members, especially in the field of cybersecurity. Though reports on the matter often praise this merging of Israel's public and private spheres, they rarely acknowledge the documented corruption within Unit 8200, the unit's dark past in recruiting felons and even pedophiles to join its ranks, or the danger posed by having companies directly linked to foreign intelligence being given access to the U.S. government's most classified and sensitive systems and data.

The last omission is particularly troubling given that Israeli intelligence has not only been caught aggressively using private tech companies to spy on U.S. federal agencies and networks, but also intercepting the private communications of at least two U.S. presidents and using a notorious pedophile to sexually blackmail American politicians.

As was mentioned in the first installment of this series, Cybereason's CEO Lior Div offers a clear example of this worrisome bridge between Israel's public and private sector, as Div has openly stated that he views his work at Cybereason as a "continuation" of his service to Israeli military intelligence, where he led offensive cyberattacks against other nations.

Given Div's past statements and his company's clear ties to both Israeli and U.S. intelligence, Cybereason's simulation of the 2020 U.S. election — which involved terrorist attacks and led to the election's cancellation and the imposition of martial law — is highly concerning. This is particularly so considering that Cybereason's investors have direct ties to individuals who would benefit from the election's cancellation and also considering the clear narrative that has emerged in recent months regarding how the coming election will inevitably fall victim to tech-driven "chaos" in coming months.

The clear overlap between Cybereason's simulation and the intelligence-driven media narrative is clear cause for concern, especially considering that the technologies that they highlight as ultimately upending the election are dominated by the very same intelligence agencies simulating and crafting that narrative.

The keyword that has been used to describe the end result of both Cybereason's simulation and the prevailing media narrative regarding the 2020 election is "chaos," chaos so imminent, widespread and unruly that it will shake American democracy to its core.

What has been left unsaid, however, is that a government's solution to "chaos" is always the imposition of "order." This means that — whatever "chaos" ultimately ensues prior to or on election day — will result in a government response that will do much more to crush freedom and undermine democracy than any act of foreign meddling has, be it real or imagined.