How Government and Media Are Prepping America for a Failed 2020 Election

Russia, China and Iran are already being blamed for using tech to undermine the 2020 election. Yet, the very technologies they are allegedly using were created by a web of companies with deep ties to Israeli intelligence.

BY **WHITNEY WEBB** JULY 15, 2020 32 MINUTE READ

As World War II drew to a close in Europe, British philosopher Bertrand Russell wrote that "neither a man nor a crowd nor a nation can be trusted to act humanely or to think sanely under the influence of a great fear."

Though numerous examples in the post-World War II era have proven Russell's point, perhaps one of the best examples was the U.S. public's willingness to swallow lie after lie about Saddam Hussein's Iraq due to the climate of fear that followed the September 11 attacks. Those lies, propagated by dubious intelligence, government officials and a compliant media, resulted in catastrophes – large and small, both abroad and at home.

Today, an analogous narrative is being crafted by many of the same players – both in media and government – yet it has avoided scrutiny, even from independent media.

Over the past several months and with a renewed zeal in just the last few weeks, anonymous intelligence officials, dubious "experts" and establishment media outlets have crafted a narrative about the coming "chaos" of the 2020 election, months before it takes place. Per that narrative, certain state actors will use specific technologies to target the "American mind" in order to undermine the coming presidential election. The narrative holds that those efforts will be so successful that the U.S. will never recover as a democracy.

Though these anonymous government sources and their stenographers have already named the countries who will be responsible and the technologies they will use, they also admit that no evidence yet exists to back up these claims, meaning they are — at best — pure speculation.

Headlines such as "Hackers Are Coming for the 2020 Election — And We're Not Ready," "Basically Every US National Security Leader Is Warning About Foreign Interference In The 2020 Election," and "U.S. intel agencies: Russia and China plotting to interfere in 2020 election" have become increasingly common, despite no available evidence, as have warnings that the American public is defenseless against the old scourge of "fake news" and the new scourge of "deep fakes." Some media reports have gone so far to say that *actual* foreign meddling isn't even necessary as merely the *fear* of foreign meddling could be enough to upend the American political system beyond repair.

Historically, the goal of such fear-inducing narratives has been the trading of civil liberties for increased security, or rather, the *appearance* of increased security. Yet, when the need for security is felt due to a fear that is based on government-driven speculation and not on evidence, the goal of that narrative is not about protecting the public from a real, tangible threat but instead about the consolidation of power by the very groups responsible for crafting it — in this case, the intelligence community and other key players in the national security state.

However, what is particularly odd about this narrative surrounding imminent "chaos" and meddling in the upcoming 2020 election is the fact that, not only have the instruments of said meddling been named and described in detail, but their use in the election was recently simulated by a company with deep ties to both U.S. and Israeli intelligence. That simulation, organized and run by the Israeli-American company Cybereason, ended with scores of Americans dead, the cancellation of the 2020 election, the imposition of martial law and a spike in fear among the American populace.

Many of the technologies used to create that chaotic and horrific scenario in the Cybereason simulation are the very same technologies that U.S. federal officials and corporate media outlets have promoted as the core of the very toolkit that they claim *will* be used to undermine the coming election, such as deep fakes and hacks of critical infrastructure, consumer devices and even vehicles.

While the narrative in place has already laid the blame at the feet of U.S. rival states China, Russia and Iran, these very technologies are instead dominated by companies that are tied to the very same intelligence agencies as Cybereason, specifically Israeli military intelligence.

With intelligence agencies in the U.S. and Israel not only crafting the narrative about 2020 foreign meddling, but also dominating these technologies and simulating their use to upend the coming election, it becomes crucial to consider the motivations behind this narrative and if these intelligence agencies have ulterior motives in promoting and simulating such outcomes that would effectively end American democracy and hand almost total power to the national security state.

Media, intelligence foreshadow tech-powered doom for 2020

Even though the 2020 U.S. election is still months away, a plethora of media reports over the past six months (and even before then) have been raising concern after concern about how the U.S. election is still so vulnerable to foreign meddling that such meddling is essentially an inevitability.

Part of the reason for the recent pick-up in fear mongering appears to have been the release of a joint statement issued by key members of the Trump administration last November. That statement, authored by Attorney General Bill Barr, Defense Secretary Mark Esper, acting DHS Secretary Kevin McAleenan, acting Director of National Intelligence Joseph Maguire, FBI Director Christopher Wray, NSA Director Gen. Paul Nakasone, and Cybersecurity and Infrastructure Security Agency (CISA) Director Christopher Krebs, claimed that foreign interference in 2020 was imminent despite admitting that there is no evidence of interference having taken place:

Our adversaries want to undermine our democratic institutions, influence public sentiment and affect government policies. ***Russia, China, Iran, and other foreign malicious actors all will seek to interfere in the voting process or influence voter perceptions****. Adversaries may try to accomplish their goals through a variety of means, including* ***social media campaigns, directing disinformation operations or conducting disruptive or destructive cyber-attacks*** *on state and local infrastructure.*

While at this time ***we have no evidence*** *of a compromise or disruption to election infrastructure that would enable adversaries to prevent voting, change vote counts or disrupt the ability to tally votes, we continue to vigilantly monitor any threats to U.S. elections (emphasis added)."*

Despite the key caveat of there being no evidence at the time the statement was issued, media reports used the statement to claim that foreign interference in 2020 was imminent, such as in these reports from *BuzzFeed*, *ABC News*, and *Newsweek*.

In addition to the reports that have cast the involvement of state actors — namely Russia, Iran and China — as assured despite no evidence, other reports have made the claim that this allegedly imminent interference will inevitably be successful, largely due to claims that the tactics used will rely heavily on technology that the U.S. can't hope to successfully counter. *CSO Online*, an online news outlets that provides news, analysis and research on security and risk management, recently warned that "fixing America's voting and election infrastructure problems is a long-term proposition, one that won't be fixed in time for the election in November" while the *New York Times* warned of imminent chaos and that "stealthier" malevolent foreign actors had already created the foundation for "an ugly campaign season marred by hacking and disinformation." *Wired* claimed last year that U.S. election security "is still hurting at every level."

In another example, *Rolling Stone* published an article earlier this month with the headline "Hackers Are Coming for the 2020 Election — And We're Not Ready," which claims that "the reality is that: "We've made progress since the last election — but we're much less secure than we should be." The article goes on to say that claim that the goal isn't necessarily to hack voting machines or change results, but "to merely create the impression of an attack as a way to undermine our faith in the electoral process."

It continues:

The target is the minds of the American people," says Joshua Geltzer, a former counterterrorism director on the National Security Council. "In some ways, we're less vulnerable than we were in 2016. In other ways, it's more." Nearly every expert agrees on this: The worst-case scenario, the one we need to prepare for, is a situation that causes Americans to question the bedrock of our democracy — free and fair elections."

Well before this type of rhetoric made its way into the U.S. media, Israeli intelligence-linked tech firm Cybereason claiming in a release on its website that "messing with a voter's mind" would have a bigger impact than changing vote totals, even before the 2016 election. That release, published by Cybereason prior to the last presidential election, was authored by the company's CEO, Lior Div, who used to lead offensive hacking operations against nation-states for Israeli military intelligence.

Notably, of all of these media reports, there is a clear consensus that one of the main tactics that will soon be used to meddle in the coming U.S. election will be the use of so-called "deep fakes." Deriving its name from a combination of "deep learning" and "fake," deep fakes involve video and audio that has been manipulated using artificial intelligence (AI) to create media that appears to be authentic, but is not. Concern about its use in the upcoming election has spurred not only a wealth of media reports on the matter but has prompted both the U.S. military and Congress to take action to limit its potential misuse.

One thing that stands out about the media narrative regarding election meddling and deep fakes is that several news organizations have published articles that state that deep fakes *will* be used to undermine the 2020 election, as opposed to stating that they could be used or that they are a phenomenon worthy of attention (though some reports have taken this more measured approach).

The reason for this level of confidence may owe to statements made by prominent U.S. intelligence officials last year, including those made by Dan Coats, the former Director of National Intelligence (DNI), who claimed in the 2019 Worldwide Threat Assessment for the U.S. Intelligence Community that deep fakes and other hi-tech forms of fake media would be used to disrupt the 2020 election. Coats specifically stated:

Adversaries and strategic competitors probably will attempt to use deep fakes or similar machine-learning technologies to create convincing—but false—image, audio, and video files to augment influence campaigns directed against the United States and our allies and partners."

Since Coats made the warning, numerous media reports have promoted the concern with little scrutiny, representing just one of the numerous times in U.S. history where narratives first authored by U.S. intelligence are subsequently promoted heavily by U.S. media, even when the claim made by intelligence officials is speculative, as it is in this case. Indeed, the narratives being promoted with respect to the 2020 election involve many of the same intelligence agencies (American and Israeli) and media outlets who promoted claims that were later proven false about "weapons of mass destruction" in Iraq prior to the 2003 invasion, among other pertinent examples.

Notably, deep fakes figured prominently and was the tool most used by malevolent hackers in Cybereason's 2020 election simulation, which saw both video and audio-only deep fakes used to spread misinformation on national and local TV channels in order to impersonate police officers and election officials and to create fake bomb threats by posing as the terror group Daesh (ISIS). Cybereason

also happens to be a partner of the organization funding the most well-known creator and producer of deep fakes in the world, an organization that — much like Cybereason itself — is openly tied to Israeli intelligence.

Aside from deep fakes, other technologies weaponized in Cybereason's election simulation have also been the subject of several media reports, such as the hacking of Internet of Things (IoT) devices and appliances and even the hacking of vehicles that have some form of internet connectivity. In the Cybereason simulation, IoT hacks were used to cut power to polling stations and disseminate disinformation while vehicles were hacked to conduct terror attacks against civilians waiting in line to vote, killing several and injuring hundreds.

Most media reports have claimed that these technologies will be part of the coming "explosion" in cyber warfare in 2020 and do not specifically link them to imminent election meddling. Others, however, have made the link to the election explicit.

Naming the culprits in advance

In addition to the apparent consensus on *how* foreign meddling will occur during the 2020 election, there is also agreement regarding *which* countries will be responsible. Again, this is largely based on statements made by U.S. national security officials. For instance, the joint statement issued last November by the DOJ, DOD, DHS, DNI, FBI, NSA, and CISA regarding 2020 election security, states that "Russia, China, Iran, and other foreign malicious actors all will seek to interfere in the voting process or influence voter perceptions" before adding "at this time we have no evidence."

Similarly, the 2019 Worldwide Threat Assessment for the U.S. Intelligence Community, written by then-Director of National Intelligence Dan Coats, names these same three countries in relation to imminent 2020 election interference and states that their interference in the 2020 election is "almost certain." The assessment adds the following about each nation:

- Russia: "Russia's social media efforts will continue to focus on aggravating social and racial tensions, undermining trust in authorities, and criticizing perceived anti-Russia politicians."
- China: "China will continue to use legal, political, and economic levers—such as the lure of Chinese markets—to shape the information environment. It is also capable of using cyber attacks against systems in the United States to censor or suppress viewpoints it deems politically sensitive."
- Iran: "Iran, which has used social media campaigns to target audiences in both the United States and allied nations with messages aligned with Iranian interests, will continue to use online influence operations to try to advance its interests."

Coats' assessment was enough to spawn numerous stories on the imminent threat that these three nations pose to the 2020 election, with headlines such as "U.S. intel agencies: Russia and China plotting to interfere in 2020 election."

The vast majority of warnings regarding future election interference have come from U.S. intelligence officials with a dubious record of trustworthiness and a history of using the media to spread propaganda and disinformation, most famously through Operation Mockingbird. Most — if not all — of the recent and numerous articles on imminent interference rely heavily on claims made by the two aforementioned government documents, documents crafted by U.S. intelligence agencies for public consumption, as well as claims made by anonymous U.S. officials.

A recent *New York Times* article, for example, titled "Chaos Is the Point': Russian Hackers and Trolls Grow Stealthier in 2020," is based almost entirely on "interviews with dozens of officials and experts," though the only government official named in the article is Shelby Pierson, the intelligence community's election threats executive. The most quoted experts named in the article are Ben Nimmo, formerly of the hawkish, NATO-funded Atlantic Council and now with Graphika, and Laura Rosenberger, director of the neoconservative-created Alliance for Securing Democracy. The article nonetheless cites "American officials" and "current and former officials" several times to make claims about imminent election interference that paint a bleak picture of the current election season.

A recent article from *The Hill* relies on the acting head of DHS, Chad Wolf, as its only source, citing Wolf's claim that "we fully expect Russia to attempt to interfere in the 2020 elections to sow public discord and undermine our democratic institutions" amid other warnings that Wolf gave about Chinese and Iranian cyber threats to U.S. elections. Other articles, including one titled "Russia, China plan to adjust their tactics to hack, influence 2020 elections" cite only Shelby Pierson of the U.S. intelligence community as its source for that headline's claim. Another titled "Russia isn't the only threat to 2020 elections, says U.S. intel" cites only anonymous U.S. intelligence officials, as the headline suggests.

Though Russia and China have consistently been named as the most likely election meddlers, reports have also been drumming up the likelihood that Iran will emerge as 2020's foreign meddler of choice, especially in the months prior to and weeks after the killing of Iranian General Qassem Soleimani by the Trump administration. A recent "informal poll" conducted by the *Washington Post*asked hawkish think tank fellows, employees at companies like Raytheon and current and former federal officials if Iran would likely retaliate against the U.S. via cyberattack. The *Post* ran the results of the poll under the headline "Get ready for serious cyberattacks from Iran, experts say."

Despite the media's numerous warnings of imminent and "serious" cyber-retaliation from Iran, the only cyberattack attributed to the country after Soleimani's death was the vandalism of the Federal Depository Library Program website, a rather benign act that was nevertheless blasted across headlines such as "US government website hacked with pro-Iranian messages, image of bloodied Trump." The U.S. government is quoted in that article as saying that "At this time, there is no confirmation that this was the action of Iranian state-sponsored actors."

Also notably absent from media reports is the fact that WikiLeaks revealed in 2017 that the CIA had stockpiled a library of "stolen" cyberattack techniques produced in other nations, including Russia and Iran. Those revelations, part of the Vault 7 release, revealed that the CIA's UMBRAGE group was capable of "misdirect[ing] attribution [for cyberattacks actually done by the CIA] by leaving behind the 'fingerprints' of the groups that the attack techniques were stolen from." In other words, the CIA was more than capable of conducting "false flag" cyber attacks and blaming them on foreign actors.

Notably, one of the viruses being blamed on Iran for cyberattacks targeting the U.S. ahead of the 2020 election — called Shamoon — was "stolen" by the CIA's UMBRAGE and cited in the WikiLeaks release.

Conflict of interest-ridden Microsoft "defends democracy"

Last year saw the tech behemoth Microsoft join the effort to blame foreign state actors, specifically Iran, for cyberattacks against the U.S. This helped to bolster assertions that had largely originated with a handful of U.S. intelligence officials and hawkish, neoconservative-aligned think tanks as media reports on Microsoft's related claims treated the company as an independent private sector observer.

Yet, as *MintPress* investigations have revealed, Microsoft has clear conflicts of interest with respect to election interference. Its "Defending Democracy" program has spawned tools like "NewsGuard" and "ElectionGuard" that it claims will help protect U.S. democracy, but — upon closer examination — instead have the opposite effect.

Last January, *MintPress* exposed NewsGuard's neoconservative backers and how special interest groups were backing the program in an effort to censor independent journalism under the guise of the fight against "fake news." Subsequent investigations revealed the risk that Microsoft's ElectionGuard poses to U.S. voting machines, which it claims to make more secure and how the platform was developed by companies closely tied to the Pentagon's infamous research branch DARPA and Israeli military intelligence Unit 8200.

ElecionGuard software has since been adopted by numerous voting machine manufacturers and is slated to be used in some Democratic Primary votes. Notably, the push for the adoption of ElectionGuard software has been spearheaded by the recently created Cybersecurity and Infrastructure Security Agency (CISA), which is the federal agency tasked with overseeing election security and is headed by Christopher Krebs, a former high level Microsoft executive.

In recent months, Microsoft has also been at the center of claims that Iran attempted to hack U.S. presidential campaigns ahead of 2020 as well as claims that Iran plans to target the U.S. power grid and other critical infrastructure with cyberattacks.

Last October, Microsoft penned a blog post discussing a "threat group" it named Phosphorus that they "believe originates from Iran and is linked to the Iranian government." The post went on to claim that Phosphorus attempted to target a U.S. presidential campaign, which later media reports claimed was President Trump's re-election campaign. Microsoft concluded that the attempt was "not technically sophisticated" and ultimately unsuccessful, but felt compelled to disclose it and link it to Iran's government.

Though it provided no evidence for the hack or its reasons for "believing" that the attack originated from Iran, media reports treated Microsoft's declaration as proof that Iran had begun actively meddling in the 2020 election. Headlines such as "Iranian Hackers Target Trump Campaign as 2020 Threats Mount," "Iran-linked Hackers Target Trump 2020 Campaign, Microsoft says", "Microsoft: Iran government-linked hacker targeted 2020 presidential campaign" and "Microsoft Says Iranians Tried To Hack U.S. Presidential Campaign," were blasted across the front pages of American media. None of the reports scrutinized Microsoft's claims or noted the clear conflict of interest Microsoft had in making such claims due to its efforts to see its own ElectionGuard Software adopted nationwide.

Media reports also left out the fact that Microsoft is a major government contractor for the U.S. intelligence community and the Pentagon. Notably, the Trump campaign, which Microsoft said was the target of this attack, was later identified as the only major presidential campaign using Microsoft's "AccountGuard" software, part of its dubious "Defending Democracy" program that also spawned NewsGuard and ElectionGuard. AccountGuard claims to protect campaign-linked emails and data from hackers.

Microsoft surfaced not long after, again claiming that Iran was maliciously targeting the United States' civilian infrastructure. This subsequent claim was first published by *Wired* and later covered by other outlets. Those reports cite a single person, Microsoft security researcher Ned Moran, who claimed that an Iran-backed hacking group called APT33 was targeting the U.S. "physical control systems used in electric utilities, manufacturing, and oil refineries."

"They're trying to deliver messages to their adversaries and trying to compel and change their adversaries' behavior," Moran told *Wired*. Moran also stated that "Microsoft **hasn't seen direct evidence** of APT33 carrying out a disruptive cyberattack rather than mere espionage or reconnaissance, it's seen incidents where the group has **at least laid the groundwork** for those attacks (emphasis added)."

Cybereason helps craft the narrative

While U.S. intelligence officials and media outlets alike have been largely responsible for setting the narrative that imminent meddling will be conducted by Russia, China and Iran, key components of that narrative, particularly with respect to China and Iran, have been laid by Cybereason, a company that recently ran 2020 doomsday election simulations and that has close ties to the intelligence communities of both the U.S. and Israel.

Shortly after the killing of Iranian General Qassem Soleimani earlier this month, an operation conducted in concert with Israeli intelligence, Cybereason warned that Iran could imminently retaliate with a cyber threat and quoted its own employees who explained what and how Iran would likely target in retaliation. Cybereason's CSO Sam Curry, who actively participated in the firm's 2020 doomsday election simulations, stated:

*This means that Iran's "forceful revenge" response is likely to be less about the flash and all about the bang. If you have connected systems that are responsible for kinetic world effects, like **ICS systems and critical infrastructure around water, energy or vital services**, it's time to pay attention. Iran and the US are engaged in Cyber brinksmanship, which means that **the gloves are off as Iran picks it's targets** (emphasis added)."*

Cybereason also quoted visiting fellow for the National Security Institute and former advisor to the U.S. Secret Service (which participated in Cyberaeson's election simulations), Anne Marie Zettlemoyer, who claimed that Iran could soon target Wall Street and critical U.S. infrastructure like the power grid:

An attack against the financial systems can be devastating economically and weaken the confidence and viability of markets. However, we cannot ignore the physical consequences and manifestations that can

come from a cyberattack, particularly against critical infrastructure like energy and industry control systems."

Cybereason's claims regarding Iran's interest in "critical infrastructure" systems likely originated with Microsoft, the claims were then parroted by the media in several reports, many of which quoted Cybereason's Sam Curry. Curry is also a contributor to major news outlets like *Forbes* where he writes about Iran's cyber warfare capabilities.

Notably, in Cybereason's recent allegations against Iran, it states that "it's clear that Iran has been preparing for future geopolitical conflict by gaining access to critical infrastructure and other important operations in the United States." It backs these claims by citing an article authored by Curry for *Forbes*. Following Soleimani's death, numerous media reports, including in the UK's *The Independent* and *ABC News*, have cited Curry as an "expert" source in claiming that Iran would retaliate with cyberattacks.

Microsoft's claims about foreign hackers and meddling — the evidence for which have never been made public but has been parroted as fact nonetheless — are frequently supported by Cybereason.

Last August, Microsoft claimed to have foiled Russian attempts at hacking two Republican-affiliated think tanks and, despite providing no evidence, Cybereason's then-senior director of intelligence services Ross Rustici was quoted as an expert in several media reports as saying that such behavior was to be expected from Russia. In one such report, Rustici stated:

We're very good at fighting the last war, but the Russians are very good at evolving their game. I suspect if they're going to do a psychological operation around the elections, the way they do it will be different than what they did in 2016. How effective the defenses we've built for what they did in 2016 will be for those attacks is yet to be seen."

None of the media reports quoting Rustici mentioned Cybereason's ties to Israeli intelligence, referring to tech firms only a "Boston-based cybersecurity company" and similar variants. Cybereason's Intelligence Group is stuffed with former and *active* members of U.S. and Israeli intelligence services and has released several reports about nation-state hacking with a focus on Russia and China.

Cybereason has also been at the forefront of claims that China has been engaged in aggressive cyberattacks against multinational companies that have also seen widespread coverage in U.S. media, despite the untransparent nature of the evidence for Cybereason's claims.

In a story that received major coverage from outlets such as *Fox News, Reuters, CNBC* and others, Cybereason unveiled what it called "Operation Soft Cell," an operation that stole mass troves of data from several global telecommunications companies. In each story, Cybereason is the sole source of the claim and declined to provide the name or location of any of the affected companies. The firm also claimed to have determined that the attack was *likely* perpetrated by someone "backed by a nation state, and is affiliated with China." It further claimed to have debriefed and coordinated responses with U.S. intelligence.

In an article for *Reuters*, Cybereason stated that "this time as opposed to in the past we are sure enough to say that the attack originated in China" while Cybereason separately told *CyberScoop* that it had "found hacking tools such as a modified web shell and a remote access trojan that are commonly associated with,

but not unique to, Chinese hackers." Despite the incongruity, media reports laid the blame squarely on China, as seen in headlines such as "Chinese spies have been sucking up call records at multinational telecoms, researchers say."

Prior to uncovering Operation Soft Cell, Cybereason had warned on its blogs in the months and years prior that China would imminently target U.S. companies. The revelation of Operation Soft Cell — which originated exclusively with Cybereason — has been used to build the case that China is openly engaged in cyberwarfare against its rival states, like the United States, and targeting "democracy itself."

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, all their secrets, their lives, their futures,” as well as a video showing Richard Nixon giving a speech he never actually gave. More recently, Canny AI was behind the viral videos immediately prior to the 2019 U.K. general electionthat 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 calledXcelerator, 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 tiesto 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.

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.

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 byNadav 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 corruptionwithin 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 pedophileto 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.

cybersecurity intelligence israel 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.

5 comments

Maricata says:
July 30, 2020 at 6:51 pm

You can add Antifa to the list along with Iran, China and Russia.
Reply

Russ says:
August 1, 2020 at 6:38 am

Thanks, Whitney, for another comprehensive and coherent piece of writing; which brings to light some of the forces, behind the scenes, that have created – and commandeered – multifarious means and measures to effectively bypass the systems of security and defense erected by countries s/a the USA. Moreover, it's quite harrowing and haunting how the recurring pattern – as you so poignantly point out – of simulation and subsequent 'event' (exs., '9/11; Covid-19; etc.) has manifested itself time-and-time again; which can't help but leave one – in recognition of the most recent simulation – walking on pins and needles these days; as they anxiously await for the appearance of the next cataclysmic 'event.'
Reply

Andy says:
November 23, 2020 at 4:59 am

So in July 2020 the TPTB supported by the MSM are constantly beating the drums about the mortal threat of foreign interference already underway with respect to the 2020 election. Yet immediately after said election, we are told by the head of the cybersecurity department at the DHS that "it was the most secure election ever". To say that is an incomprehensible shift in attitude / perception is an understatement. What changed over that 3-4 month period other than apparently the "right guy" won the election?
Reply