GlobalResearch
Center for Research on Globalization

Israel Perfecting Surveillance Tech

Leave it to the Mossad and Shin Bet to profit militarily and financially from virus.

By Philip Giraldi
Global Research, May 15, 2020

Region: Middle East & North Africa, USA
Theme: Intelligence

Israel's external spy organization Mossad and its internal espionage equivalent Shin Bet have reputations that are much larger than their actual successes, but the one area where they have excelled is electronic intelligence gathering. Recent electronic spying around the White House and other federal buildings in Washington carried out by the Israeli Embassy demonstrates that Israel does not differentiate much between friends and enemies when it conducts espionage. In fact, spying targeting the U.S. is probably its number one priority due to the fact that the Jewish state is so heavily dependent on American support that it feels compelled to learn what discussions relating to it are taking place behind closed doors.

Israeli penetration of U.S. telecommunications began in the 1990s, when American companies like AT&T and Verizon, the chief conduits of the National Security Agency (NSA) for communications surveillance, began to use Israeli-produced hardware, particularly for law enforcement-related surveillance and clandestine recording. The devices had a so-called back door, which meant that everything they did was shared with Israel. Israeli cyber-specialists even broke into classified networks with the NSA and FBI aware of what was going on but unwilling to confront "America's best ally." President Bill Clinton once quipped to Monica Lewinski that they should avoid using the Oval Office phone because someone might be listening in. He was referring to Israel.

To be sure, the Jewish state's high-tech sector has been much assisted in its effort by "own goals" provided by the United States, which allows Israel to bid on government contracts relating to national security, virtually guaranteeing that any technical innovations will be stolen and re-exported by Israeli high-tech companies. Major technology innovators like Intel, which works with the NSA, have set up shop in Israel and have publicly stated, "We think of ourselves as an Israeli company as much as a U.S. company." Vulture capitalist Zionist billionaire Paul Singer has recently been accused of steering highly paid U.S. tech sector jobs to Israel, jobs that are lost to the American economy forever.

So, Israel is a leader in using electronic resources to carry out espionage and collect information on various targets of interest. Israel is also an innovator, and its close relationship with the U.S. intelligence community (IC), most particularly the NSA, means that technologies and procedures developed by the Jewish state will inevitably show up in America.

The U.S. is in any event working hard on its own tools for managing the public, spurred by Covid-19 hysteria. Special ID cards could help track the health status of individuals. This status would be recorded and updated on a chip readable by government scanners that, by some accounts, might be either carried or even permanently embedded in everyone's body. Another plan being promoted in a joint venture by Apple and Google that appears to have

White House support involves “add[ing] technology to their smartphone platforms that will alert users if they have come into contact with a person with Covid-19. People must opt into the system, but it has the potential to monitor about a third of the world’s population” with monitoring done by central computers. Once the legal principle is established that phones can be manipulated to do what is now an “illegal search,” there are no technical or practical limits to what other tasks could also be performed.

Developments in Israel

With those steps being taken to control the movements of possibly infected citizens in mind, some recent developments in Israel are, to put it mildly, ominous. **The Jewish state is currently achieving multi-level 24/7 surveillance of everyone residing in the country conducted in real time.** Investigative reporter and peace activist **Richard Silverstein** describes in some detail why it is happening now, what it means, and how it works.

Per Silverstein, Israel, like every other authoritarian state, is currently taking advantage of the distraction caused by the coronavirus pandemic. Prime Minister **Benjamin Netanyahu,** whose political fortunes seemed to be on the wane due to three hung elections, exploited the fear of the virus to assume emergency powers and obtain Knesset approval to use a highly classified national database “compiled by the Shin Bet and comprising private personal data on every Israeli citizen, both Jewish and Palestinian. In the aftermath of 9/11, Israel’s Knesset secretly assigned its domestic intelligence agency the task of creating the database, which was ostensibly meant as a counterterrorism measure.”

The database, nicknamed “The Tool,” includes names, addresses, phone numbers, employment, and educational information but it goes well beyond that in using phone tracking data to record every phone call made by the individual to include names and numbers of those called and the geo-location of where the call was made from. Phone tracking also enabled Shin Bet to create a log of where the caller traveled in Israel and the occupied territories. Internet use, if active on the phone, was also recorded. It is as complete and total surveillance of an individual as is possible to obtain and it does not involve any human participation at all, every bit of it being done by computer.

Netanyahu publicly proclaimed his intention to use the database, stating that it would be employed to combat the coronavirus, which he described as a threat to national survival. As a result of the claimed crisis, he and his principal opponent, Blue and White party leader **Benny Gantz,** were able to come to terms on April 20 to form a “national emergency unity government” with Netanyahu as prime minister yet again.

The exploitation of the fear of the virus plus that revelation about Israel’s powerful technical tool to thwart it produced a victory for Netanyahu, who effectively portrayed himself as a strong and indispensable leader, erasing the stigma resulting from his pending trial on charges of massive corruption while in office. One of the first steps Netanyahu will reportedly take is to replace the attorney general and state prosecutor who were seeking to send him to prison, effectively taking away the threat that he might go to prison.

The exposure of the existence of the database inevitably led to charges that Netanyahu had, for personal gain, revealed Israel’s most powerful counterterrorism weapon. There were also concerns about the significance of the huge body of personal information

collected by Shin Bet, to include suggestions that it constituted a gross violation of civil liberties. But carefully stoked fear of the virus combined with some political deals and maneuvers meant that use of the data was eventually approved by the Knesset security committee at the end of March.

Israel, which has closed its borders, and which still has a relatively low level of coronavirus infections and deaths, has already started using the Shin Bet database while also turning the attempts to deal with the disease as something like an intelligence war. The information obtained from "The Tool" enables the police and military to determine if someone were standing near someone else for more than a few minutes. If the contact included someone already infected, all parties are placed under quarantine. Any attempt to evade controls leads to arrest and punishment of a six-month prison term plus a $1,500 fine. Armed soldiers patrolling the streets are empowered to question anyone who is out and about.

Mossad is also involved in fighting the virus, boasting of having "stolen" 100,000 face masks and also respirators from a neighboring country presumed to be the United Arab Emirates. Silverstein observes that "Israel's far-right government has militarized the contagion. Just as a hammer never met a nail it didn't want to pound, it is only natural for a national security state like Israel to see Covid-19 as a security threat just as much or more than a health threat." And when it comes to bioweapons, Israel is no *parvenu*. Ironically, the hidden story behind the "war on the coronavirus" is that Israel is itself one of the most advanced states in developing and testing biological weapons at its lab at Nes Tziona.

Returning to the emergence of "The Tool," hardline Defense Minister **Naftali Bennett** has also suggested monetizing the product by selling a "civilian version of it," to include its operating system, analytic capabilities, and setup details to foreign countries, including the United States. Israel has already successfully marketed to security agencies and governments a similar product called Pegasus, which has been described as the most sophisticated malware on the market.

Like The Tool, Pegasus does data mining and real-time analysis of individuals based on a range of collection techniques. The Israeli cyber company NSO Group that markets Pegasus was recently involved in an attempt to hack Facebook-owned secure communications system Whats-App, targeting journalists and political activists, on behalf of an unknown client. Ironically, it is believed that Facebook had earlier used NSO Group's somewhat shadowy services. Perhaps more notoriously, Pegasus was also used to monitor contacts and establish physical location in the case of journalist Jamal Khashoggi, who was murdered by Saudi intelligence agents in Istanbul.

So, Americans should beware when confronted by the new cyber-security software being promoted by Israel because the Jewish state is also exporting its own vision of a centrally controlled militarized state where all rights are potentially sacrificed for security. As whistleblower Edward Snowden has already revealed, the NSA has the capability to collect vast amounts of information on citizens. If the United States government falls for the bait and moves in the Israeli direction, using that data to enable the surveillance and manage all the people all the time, the temptation will be great to employ the new capability even if its use is not strictly speaking warranted.

And there will be no one there to say nay to the new powers, not in Congress, on the Supreme Court or in the White House. And the media will be on board, too, arguing that security against external and internal threats requires some infringements of individual

rights. It is one of the ironies of history that the United States of America, with its vast resources, large population and legacy of individual freedom, has been becoming more like its tiny militarized client state Israel. It is a tendency that must be resisted at all costs by every American who cares about fundamental liberties.

*

Note to readers: please click the share buttons above or below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

This article was originally published on American Free Press.

***Philip Giraldi** is a former CIA counter-terrorism specialist and military intelligence officer and a columnist and television commentator. He is also the executive director of the Council for the National Interest. His other articles appear on the website of "The Unz Review."*

Featured image is from American Free Press
