Articles & Op-Eds

The Rise of the Cyber-Mercenaries

Neri Zilber

Foreign Policy

September 2018

What happens when private Middle Eastern firms have cyberweapons as powerful as those owned by governments?

The first text message showed up on Ahmed Mansoor's phone at 9:38 on a sweltering August morning in 2016. "New secrets about torture of Emiratis in state prisons," it read, somewhat cryptically, in Arabic. A hyperlink followed the words. Something about the number and the message, and a similar one he received the next day, seemed off to Mansoor, a well-known human rights activist in the United Arab Emirates. He resisted the impulse to click on the links.

Instead, Mansoor sent the notes to Citizen Lab, a research institute based at the University of Toronto specializing in human rights and internet security. Working backward, researchers there identified the hyperlinks as part of a sophisticated spyware program built specifically to target Mansoor. Had he clicked on the links, the program would have turned his phone into a "digital spy in his pocket," Citizen Lab later wrote in a report—tracking his movements, monitoring his messages, and taking control of his camera and microphone.

But the big revelation in the report wasn't so much the technology itself; intelligence agencies in advanced countries have developed and deployed spyware around the world. What stood out was that Citizen Lab had traced the program to a private firm: the mysterious Israeli NSO Group. (The name is formed from the first initials of the company's three founders.) Somehow, this relatively small company had managed to find a vulnerability in iPhones, considered to be among the world's most secure cellular devices, and had developed a program to exploit it—a hugely expensive and time-consuming process. "We are not aware of any previous instance of an iPhone remote jailbreak used in the wild as part of a targeted attack campaign," the Citizen Lab researchers wrote in their report.

Israel is a world leader in private cybertechnology, with at least 300 firms covering everything from banking security to critical infrastructure defense. But while most of these firms aim to protect companies from cyberattacks, a few of them have taken advantage of the thin line between defensive and offensive cybercapabilities to provide clients with more sinister services. In the case of Mansoor, the UAE is believed to have deployed NSO tools to conduct surveillance on the country's most famous dissident. (He is now serving a 10-year prison sentence for publishing "false information" on his social media accounts.) "[T]hese companies apply techniques as sophisticated, or perhaps sometimes more sophisticated, than U.S. intelligence agencies," Sasha Romanosky, a policy researcher at the Rand Corp., wrote last year.

The privatization of this offensive capability is still in its infancy. But it raises broad concerns about the proliferation of some very powerful tools and the way governments are losing the monopoly over their use. When state actors employ cyberweapons, there is at least the prospect of regulation and accountability. But when private companies are involved, things get more complicated. Israel offers a good test case. It produces a steady supply of highly skilled cyberoperators who learn the craft during their military service in one of the country's elite signals intelligence units—Unit 8200 is the best known among them—and then go on to work in the private sector. Nadav Zafrir, a retired brigadier general and former commander of Unit 8200, said even soldiers who spend their service defending Israel from cyberattacks end up knowing something about how to attack the other side. "In order to mitigate the gap between defense and offense, you have to have an attacker's mindset," he said.

The Mansoor case was not an isolated one. Up to 175 people have been targeted by the NSO Group's spyware since 2016, according to Citizen Lab, including human rights workers and dissidents. Other Israeli firms offer similar products. "There's no way around it: In order to provide network defense, you need to map vulnerabilities," said Nimrod Kozlovski, an adjunct professor at Tel Aviv University and a lawyer specializing in cybersecurity. "It's built from [Israel's] deep knowledge of these weaknesses and attack methods. We're deeply familiar with what targets look like."

Take the most famous of these alleged targets: Iran's uranium enrichment facility at Natanz, where Unit 8200, in collaboration with the U.S. National Security Agency (NSA), reportedly carried out an attack in 2009-2010. They were apparently able to introduce a computer virus—called Stuxnet—into the facility despite it having an air gap in place, meaning that the facility was physically disconnected from the wider internet. The virus targeted the operating system for Natanz's uranium centrifuges, causing them to speed up wildly and break; the monitoring

system was also apparently hacked so that the damage, when it happened, initially went unnoticed by the Iranians.

It's probably no coincidence that many Israeli cyberdefense firms market products aimed at forestalling Stuxnet-style attacks on critical infrastructure. These firms include Aperio Systems, which is headed by a former intelligence officer named Liran Tancman. Aperio, in fact, has a product that detects data manipulation—a "truth machine," as Tancman puts it—in sensor readings at industrial plants.

Stuxnet is name-checked repeatedly by experts in the field and with good reason: It was a highly successful cyberattack against a state actor that caused real physical damage. Yet Stuxnet may already be outdated as an analytical touchstone. As Gabriel Avner, an Israel-based digital security consultant, said, "A decade in tech is an eternity." These days, the attack surface is growing, said Zafrir, the former Unit 8200 commander who now runs Team8, a combination venture capital fund, incubator, and ideas lab. The development that worries him and other experts most is the proliferation of the internet of things.

"Everything is becoming a computer—your phone, your fridge, your microwave, your car," said Bruce Schneier, an expert on cyber-related issues at Harvard University. The problem is that the internet, which came of age in the 1970s and 1980s, was never designed with security in mind. So everyone is now scrambling to play catch-up, patching holes in both information systems (e.g., software programs) and operating systems (e.g., physical industrial plants) that are outdated, poorly written, or simply insecure. "Attacks always get faster, easier, and better," added Schneier, the author of *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*.

Does this mean we're all doomed? The short answer is no—at least, probably not. Thus far, apart from Stuxnet, the most successful reported instances of a cyberattack causing widespread physical damage have taken place in Ukraine and Estonia. Although these attacks—against power grids, financial institutions, and government ministries—caused real harm, they were nevertheless identified and rectified relatively quickly. None of the doomsday scenarios that experts and pundits like to warn about—such as hackers seizing control of a nuclear weapon or a commercial airliner or malware causing Wall Street to collapse—has materialized.

Part of the explanation is that "state-sponsored hackers will always have more resources," Tancman said. "The question is how far ahead of the [nonstate actors] you're running. A 'cyber-nuke weapon' today won't be relevant in a year or two. The issue is the pace of development between attackers and defenders. Always keep running."

If part of the danger comes from the blurriness of the line that separates cyberdefense and cyberoffense, another part comes from the almost nonexistent distinction between the private and public spheres online. In July, for example, Israeli authorities announced multiple indictments against a former employee of NSO Group, alleging that he had stolen sensitive proprietary code on his way out of the firm. But the unnamed employee was also charged with attempting to undermine national security: He had apparently tried to sell the information for $50 million in cryptocurrency to a foreign buyer on the darknet, the vast anonymous hinterland of the internet inaccessible by regular search engines.

This incident, quickly detected by the firm, is just one case among many that shows how intimately the private and public spheres are linked in cyberwarfare. Capabilities that were once the sole province of governments frequently find their way into private—often criminal—hands.

The Stuxnet virus code is now publicly available. In 2013, a cyberweapon developed by the NSA that exploited vulnerabilities in Microsoft Windows was stolen by hackers—possibly Russian—and posted online; in May 2017, other hackers—possibly North Korean—then used the tool to launch a worldwide ransomware attack. The attack, called WannaCry, is believed to have infected 200,000 computers in more than 150 countries, including major parts of the British National Health Service, before it was rolled back. In a separate 2013 case, Mandiant, a private U.S. cybersecurity firm, proved that hackers affiliated with the Chinese military were targeting U.S. corporations and government agencies. And in 2015, Unit 8200 reportedly hacked into Kaspersky Lab, a global leader in anti-virus software, and discovered that the private company had been acting as a back door for Russian intelligence into its clients, including two dozen U.S. government agencies.

"In the physical world of warfare, what is public has always been clear: tanks, Iron Dome [missile defense systems], F-16s," said Rami Ben Efraim, a retired Israeli brigadier general and the founder of BlueOcean Technologies, an offensive cybersecurity firm. "In cyber today, it's complicated." Critical infrastructure, such as power utilities or water treatment plants, may be privately owned, as is often the case in the United States, but would cause national damage if its systems crashed. Mobilization messages for Israeli reserve forces in wartime go through privately held telecom networks. And the internet of things—which has connected so many of our consumer products—has also created massive vulnerabilities.

"If you want to take down a plane, if you want to ground air power, you don't go through the front door, the cockpit," said Ben Efraim, a former fighter pilot. "You go after the airport...You go after the logistics systems. You go after the iPads the pilots take home." There are no "stand-alone entities anymore—everything is part of a network," Ben Efraim added. As Lithuania's vice minister of defense, Edvinas Kerza, told me last fall in the capital of Vilnius, alluding to Russia's actions against other former Soviet states: "The attacks come from within—banks down, government not responsive, general instability...'It's fine to set up a border,' they say. 'We'll come from the inside.'"

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," Avner, the security consultant, said by way of emphasis.

In a world where Israel's vaunted internal security agency, the Shin Bet, recently launched a private start-up accelerator, such private-public collaboration will only grow. Indeed, it must if it is to keep up with rapid developments in areas such as artificial intelligence, machine learning, and other breakthroughs in computational power.

Cyberwar has not only blurred the lines between offense and defense; it has also blurred the notion of sovereign property when it comes to technological development—namely what, exactly, constitutes an Israeli (or U.S. or Chinese) company. The internet has eclipsed borders, and cyberwarfare is no exception. As Harvard's Schneier put it, the "chips are made in X, assembled in Y, and the software is written all over the world by 125 different nationals." Such fluidity is especially common in Israel, where deep-pocketed foreign firms have established research and development outposts and bought up local start-ups.

While the international nature of computer technology confers many benefits, it also makes it hard to ascertain the origin of a cyberattack. That lack of attribution then makes it harder for governments to respond, and the lack of a threat of reprisal makes deterrence difficult, if not impossible. "That is why cyberweapons have emerged as such effective tools for states of all sizes: a way to disrupt and exercise power or influence without starting a shooting war," David Sanger wrote in a *New York Times* article adapted from his book *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*.

While the private sector may be able to pay its people more, drawing talent—and technological prowess—away from public service, the government still holds one trump card: the law. Which brings us back to the NSO Group and Mansoor, the Emirati dissident. In order to legally sell the offensive cyberweapon used to target him, NSO would have needed permission from Israel's weapons export regulator, which sits in the Defense Ministry. In this way at least, cyberweapons are as tightly regulated as other weapons systems sold by the Israelis to foreign governments. And the clients are solely governments.

"Selling such systems to nongovernments, like a company or oligarch, is completely illegal," said Yuval Sasson, a partner specializing in defense exports at Meitar, one of Israel's leading law firms. "Just like with a drone or assault rifle, the regulator looks at the end user: the identity of the government and what it does. Functionality is a central test." In the case of the UAE and Mansoor, some officials within the regulator's office counseled against selling such a system to an Arab state, according to the Israeli daily *Yedioth Ahronoth*. It reported that the cyberweapon the regulators ultimately approved was weaker than the one proposed by NSO and said some officials in the Defense Ministry opposed the deal because the technology was being sold to an Arab country. "It's a scandal that they gave a permit like this," the newspaper quoted a senior official at the ministry as saying.

NSO, for its part, said in a statement that it complies with all relevant laws and that it "does not operate the software for its clients, it just develops it." That is a disingenuous distinction, perhaps, but it offers another example of the offense-defense and private-public conundrums: The same private cybertools deployed against perceived enemies of the state, such as journalists and dissidents, can be, and are, used to interdict narcos and terrorists as well. Indeed, in 2016 the FBI hired a separate Israeli firm, Cellebrite, to break into the iPhone of one of the terrorists involved in the 2015 San Bernardino, California, attack with a different cybertool (after Apple refused). Cellebrite reportedly sells its products in more than 100 countries.

While some critics blame Israel for rogue behavior, the country is no outlier; there are few saints in the global weapons trade, even among Western democracies. It is in the interest of Israeli firms to comply with the law, avoid abuses, and prevent technology from falling into the wrong hands. As Avner put it, "There's a lot of money to be made, and they can do it legally. Why be in the shadows?"

The upshot is that NSO wasn't operating in the shadows. The Israeli government approved the sale by a private company of an advanced cyberweapon to an Arab government with which it has intelligence and security exchanges. That decision was symbolic of how technology, warfare, and politics have changed dramatically in just a few short years. Espionage, information operations, and military attacks have been with us forever; so have private actors selling weapons all around the world (including, in recent decades, many former Israeli military personnel). The difference now is the reach and speed of these new cybertools and their easy proliferation. A "cyberarms race of historic but hidden proportions has taken off," according to Sanger—and the race is global. The potential downside is obvious: an arms race with no rules or norms and with no clear front lines. But there is no going back.

"We need to be humble. We're only starting to understand it," Ben Efraim said. "But it's a real revolution. A hundred years ago, there was no air element to warfare. Now it's a critical component of any military." "Cyber is bigger than even that," he said. "Today, you open your eyes in the morning—you're in it."

Neri Zilber is an adjunct fellow with The Washington Institute and coauthor (with Ghaith al-Omari) of the paper State with No Army, Army with No State: Evolution of the Palestinian Authority Security Forces, 1994-2018.
This article originally appeared in the September 2018 issue of Foreign Policy magazine.