MOVE OVER NSO

Meet Toka, the Most Dangerous Israeli Spyware Firm You've Never Heard Of

The mainstream media's myopic focus on Israel's Pegasus spyware and the threats it poses means that other companies, like Toka, go uninvestigated, even when their products present an even greater potential for abuse and illegal surveillance.

by Whitney Webb

July 21st, 2021

By Whitney Webb Whitney Webb

LONDON – This past Sunday, an investigation into the global abuse of spyware developed by veterans of Israeli intelligence Unit 8200 gained widespread attention, as it was revealed that the software – sold to democratic and authoritarian governments alike – had been used to illegally spy on an estimated 50,000 individuals. Among those who had their communications and devices spied on by the software, known as Pegasus, were journalists, human rights activists, business executives, academics and prominent political leaders. Among those targeted political leaders, per reports, were the current leaders of France, Pakistan, South Africa, Egypt, Morocco and Iraq.

The abuse of Pegasus software in this very way has been known for several years, though these latest revelations appear to have gained such traction in the mainstream owing to the high number of civilians who have reportedly been surveilled through its use. The continuation of the now-years-long scandal surrounding the abuse of Pegasus has also brought considerable controversy and notoriety to the Israeli company that developed it, the NSO Group.

While the NSO Group has become infamous, other Israeli companies with even deeper ties to Israel's intelligence apparatus have been selling software that not only provides the exact same services to governments and intelligence agencies but purports to go even farther.

Originally founded by former Israeli Prime Minister and Jeffrey Epstein associate Ehud Barak, one of these companies' wares are being used by countries around the world, including in developing countries with the direct facilitation of global financial institutions like the Inter-American Development Bank (IDB) and the World Bank. In addition, the software is only made available to governments that are "trusted" by Israel's government, which "works closely" with the company.

Despite the fact that this firm has been around since 2018 and was covered in detail by this author for *MintPress News* in January 2020, no mainstream outlet – including those that have extensively covered the NSO Group – has bothered to examine the implications of this story.

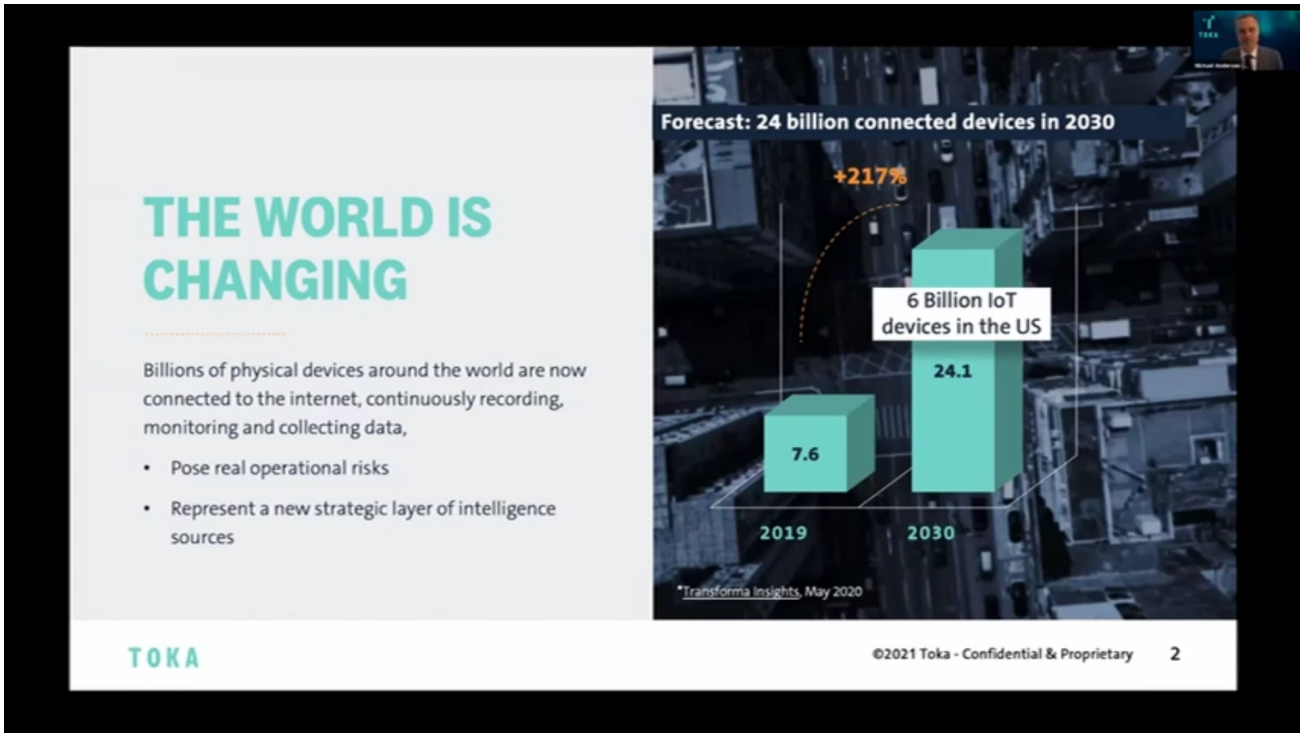
Worse than Pegasus

Toka was launched in 2018 with the explicit purpose of selling a "tailored ecosystem of cyber capabilities and software products for governmental, law enforcement, and security agencies." According to a profile of the company published in *Forbes* shortly after it launched, Toka advertised itself as "a one-stop hacking shop for governments that require extra capability to fight terrorists and other threats to national security in the digital domain."

Toka launched with plans to "provide spy tools for whatever device its clients require," including not only smartphones but a "special focus on the so-called Internet of Things (IoT)." Per the company, this includes devices like Amazon Echo, Google Nest-connected home products, as well as connected fridges, thermostats and alarms. Exploits in these products discovered by Toka, the company said at the time, would not be disclosed to vendors, meaning those flaws would continue to remain vulnerable to any hacker, whether a client of Toka or not.

Today, Toka's software suite claims to offer its customers in law enforcement, government and intelligence the ability to obtain "targeted intelligence" and to conduct "forensic investigations" as well as "covert operations." In addition, Toka offers governments its "Cyber Designers" service, which provides "agencies with the full-spectrum strategies, customized projects and technologies needed to keep critical infrastructure, the digital landscape and government institutions secure and durable."

Given that NSO's Pegasus targets only smartphones, Toka's hacking suite – which, like Pegasus, is also classified as a "lawful intercept" product – is capable of targeting *any* device connected to the internet, including but not limited to smartphones. In addition, its target clientele are the same as those of Pegasus, providing an easy opportunity for governments to gain access to even more surveillance capabilities than Pegasus offers, but without risking notoriety in the media, since Toka has long avoided the limelight.



A slide from an April 20, 2021 presentation given by Toka's VP of Global Sales, Michael Anderson

In addition, while Toka professes that its products are only used by "trusted" governments and agencies to combat "terrorism" and maintain order and public safety, the sales pitch for the NSO Group's Pegasus is remarkably similar, and that sales pitch has not stopped its software from being used to target dissidents, politicians and journalists. It also allows many of the same groups who are Toka clients, like intelligence agencies, to use these tools for the purpose of obtaining blackmail. The use of blackmail by Israeli security agencies against civilian Palestinians to attempt to weaken Palestinian society and for political persecution is well-documented.

Toka has been described by market analysts as an "offensive security" company, though the company's leadership rejects this characterization. Company co-founder and current CEO Yaron Rosen asserted that, as opposed to purely offensive, the company's operations are "something in the middle," which he classifies as bridging cyber defense and offensive cyber activities — e.g., hacking.

The company's activities are concerning in light of the fact that Toka has been directly partnered with Israel's Ministry of Defense and other Israeli intelligence and security agencies since its founding. The company "works closely" with these government agencies, according to an Israeli Ministry of Defense website. This collaboration, per Toka, is meant to "enhance" their products. Toka's direct IDF links are in contrast to the NSO Group, a company that does not maintain overt ties with the Israeli security state.

Toka's direct collaboration with Israel's government is also made clear through its claim that it sells its products and offers its services only to "trusted" governments, law enforcement agencies and intelligence agencies. Toka's Rosen has stated that Russia, China, and "other enemy countries" would never be customers of the company. In other words, only countries aligned with Israeli policy goals, particularly in occupied Palestine, are permitted to be customers and gain access to its trove of powerful hacking tools. This is consistent with Israeli government efforts to leverage Israel's hi-tech sector as a means of countering the Boycott, Divest and Sanctions (BDS) movement globally.

A profile photo of former Chief of Cyber Staff for the IDF and Toka co-founder, Yaron Rosen. Credit | Spy Legends

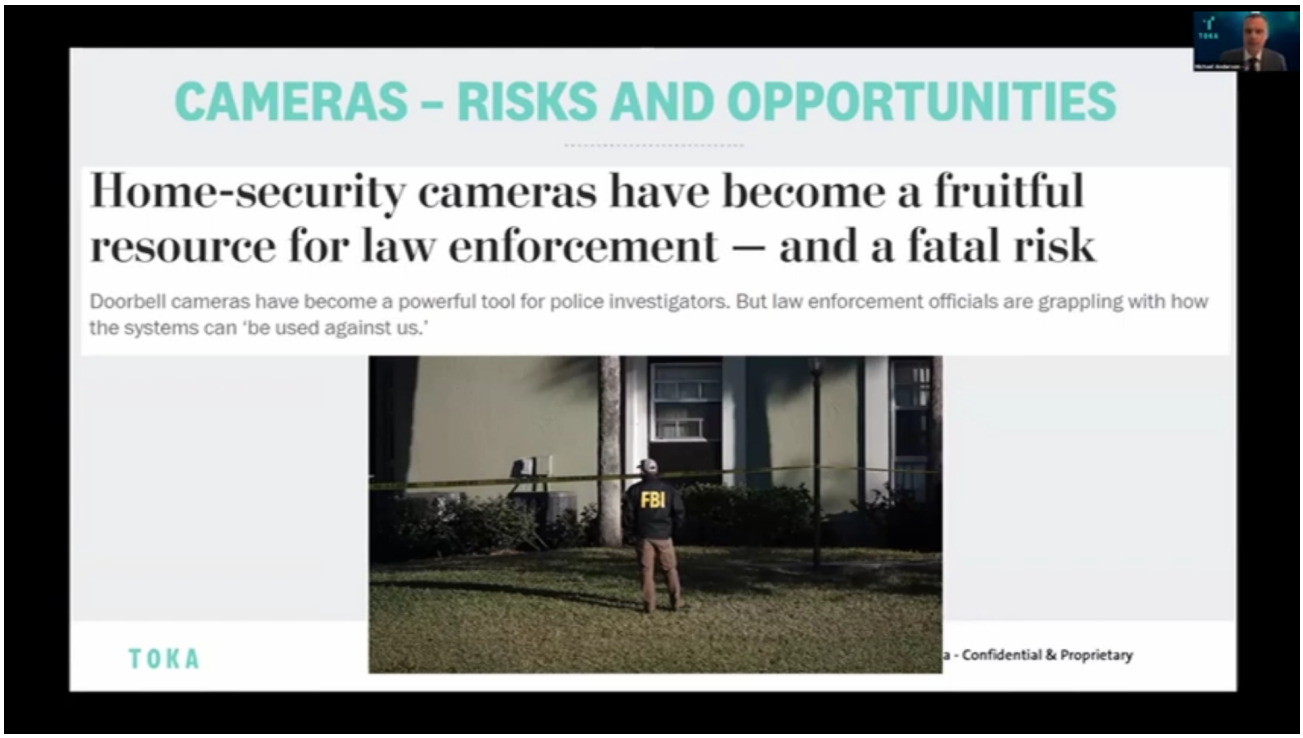
Further evidence that Toka is part of this Israeli government effort to seed foreign governments with technology products deeply tied to Israel's military and intelligence services is the fact that one of the main investors in Toka is Dell Technologies Capital, which is an extension of the well-known tech company Dell. Dell was founded by Michael Dell, a well-known pro-Israel partisan who has donated millions of dollars to the Friends of the IDF and is one of the top supporters of the so-called "anti-BDS" bills that prevent publicly employed individuals or public institutions in several U.S. states from supporting non-violent boycotts of Israel, even on humanitarian grounds. As *MintPress* previously noted, the fact that a major producer of consumer electronic goods is heavily investing in a company that markets the hacking of that very technology should be a red flag.

The government's initial admitted use of the hi-tech sector to counter the BDS movement coincided with the launch of a new Israeli military and intelligence agency policy in 2012, whereby "cyber-related and intelligence projects that were previously carried out in-house in the Israeli military and Israel's main intelligence arms are transferred to companies that, in some cases, were built for this exact purpose."

One of the reasons this was reportedly launched was to retain members of Unit 8200 engaged in military work who were moving to jobs in the country's high-paying tech sector. Through this new policy that has worked to essentially merge much of the private tech sector with Israel's national security state, some Unit 8200 and other intelligence veterans continue their work for the state but benefit from a private sector salary. The end result is that an unknown – and likely very high – number of Israeli tech companies are led by veterans of the Israeli military and Israeli intelligence agencies and serve, for all intents and purposes, as front companies. A closer examination of Toka strongly suggests that it is one such front company.

Toka — born out of Israel's national security state

The company was co-founded by Ehud Barak, Alon Kantor, Kfir Waldman and retired IDF Brigadier General Yaron Rosen. Rosen, the firm's founding CEO and now co-CEO, is the 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. Alon Kantor is the former Vice President of Business Development for Check Point Software, a software and hardware company founded by Unit 8200 veterans. Kfir Waldman is the former CEO of Go Arc and a former Director of Engineering at technology giant Cisco. Cisco is a leader in the field of Internet of Things devices and IoT cybersecurity, while Go Arc focuses on applications for mobile devices. As previously mentioned, Toka hacks not only mobile devices but also has a "special focus" on hacking IoT devices.



A slide from an April 20, 2021 presentation given by Toka's VP of Global Sales, Michael Anderson

In addition to having served as prime minister of Israel, Toka co-founder Ehud Barak previously served as head of Israeli military intelligence directorate Aman, as well as several other prominent posts in the IDF, before eventually leading the Israeli military as minister of defense. While minister of defense, he led Operation Cast Lead against the blockaded Gaza Strip in 2009, which resulted in the deaths of over 1,000 Palestinians and saw Israel illegally use chemical weapons against civilians.

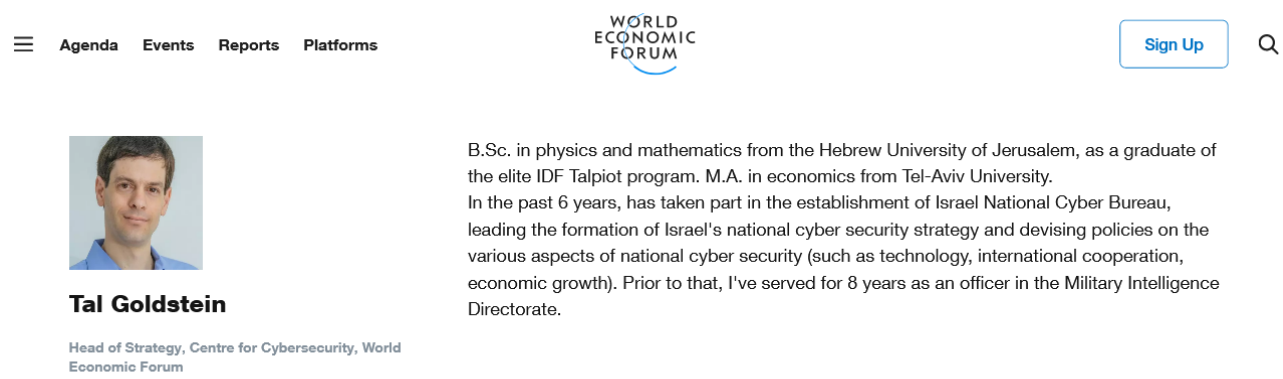
Toka is the first start-up created by Barak. However, Barak had previously chaired and invested in Carbyne911, a controversial Israeli emergency services start-up that has expanded around the world and has become particularly entrenched in the United States. Carbyne's success has been despite the Jeffrey Epstein scandal, given that the intelligence-linked pedophile and sex trafficker had invested heavily in the company at Barak's behest. Barak's close relationship with Epstein, including overnight visits to Epstein's now-notorious island and apartment complexes that housed trafficked women and underage girls, has been extensively documented.

Barak stepped away from Toka in April of last year, likely as the result of the controversy over his Epstein links, which also saw Barak withdraw from his chairmanship of Carbyne in the wake of Epstein's death. Considerable evidence has pointed to Epstein having been an intelligence asset of Israeli military intelligence who accrued blackmail on powerful individuals for the benefit of Israel's national security state and other intelligence agencies, as well as for personal gain.

Another notable Toka executive is Nir Peleg, the company's Vice President for Strategic Projects. Peleg is the former head of the Research and Development Division at Israel's National Cyber Directorate, where he led national cybersecurity projects as well as government initiatives and collaborations with international partners and Israeli cybersecurity innovative companies. Prior to this, Peleg claims to have served for more than 20 years in leading positions at the IDF's "elite technology unit," though he does specify exactly which unit this was. His LinkedIn profile lists him as having been head of the IDF's entire Technology Department from 2008 to 2011.

While at Israel's National Cyber Directorate, Peleg worked closely with Tal Goldstein, now the head of strategy for the World Economic Forum's Partnership against Cybercrime (WEF-PAC), whose members include government agencies of the U.S., Israel and the U.K., along with some of the world's most powerful companies in technology and finance. The goal of this effort is to establish a global entity that is capable of controlling the flow of information, data, and money on the internet. Notably, Toka CEO Yaron Rosen recently called for essentially this exact organization to be established when he stated that the international community needed to urgently create the "cyber" equivalent of the World Health Organization to combat the so-called "cyber pandemic."

Claims that a "cyber pandemic" is imminent have been frequent from individuals tied to the WEF-PAC, including CEO of Checkpoint Software Gil Shwed. Checkpoint is a member of WEF-PAC and two of its former vice presidents, Michael Anderson and Alon Kantor, are now Vice President for Global Sales and co-CEO of Toka, respectively.



The Wolrd Economic Forum does little to hide its partnership with former Israeli intelligence officials

Toka's Chief Technology Officer, and the chief architect of its hacking suite, is Moty Zaltsman, who is the only chief executive of the company not listed on the firm's website. Per his LinkedIn, Zaltsman was the Chief Technology Officer for then-Israeli Prime Minister Benjamin Netanyahu. Last January, when Toka was covered by *MintPress* News, his profile stated that he had developed "offensive technologies" for Israel's head of state, but Zaltsman has since removed this claim. The last Toka executive of note is Michael Volfman, the company's Vice President of Research and Development. Volfman was previously a cyber research and development leader at an unspecified "leading technology unit" of the IDF.

Also worth mentioning are Toka's main investors, particularly Entrèe Capital, which is managed by Aviad Eyal and Ran Achituv. Achituv, who manages Entrée's investment in Toka and sits on Toka's board of directors, was the founder of the IDF's satellite-based signals intelligence unit and also a former senior vice president at both Amdocs and Comverse Infosys. Both Amdocs and Comverse courted scandal in the late 1990s and early 2000s for their role in a massive Israeli government-backed espionage operation that targeted U.S. federal agencies during that period.

Despite this scandal and others in the company's past, Comverse subsidiary Verint was subsequently contracted by the U.S. National Security Agency (NSA) to bug the telecommunications network of Verizon shortly after their previous espionage scandal was covered by mainstream media. The contract was part of Operation Stellar Winds and was approved by then-NSA Director Keith Alexander, who has since been an outspoken advocate of closer Israeli-American government cooperation in cybersecurity.

In addition to Entrèe Capital, Andreessen Horowitz is another of Toka's main investors. The venture capital firm co-founded by Silicon Valley titan Marc Andreessen is currently advised by former Secretary of the Treasury Larry Summers, a close friend of the infamous pedophile Jeffery Epstein. Early investors in Toka that are no longer listed on the firm's website include 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.

In light of the aforementioned policy of Israel's government to use private tech companies as fronts, the combination of Toka's direct Israeli government ties, the nature of its products and services, and the numerous, significant connections of its leaders and investors to both Israeli military intelligence and past Israeli espionage scandals strongly suggests that Toka is one such front.

If this is the case, there is reason to believe that, when Toka clients hack and gain access to a device, elements of the Israeli state could also gain access. This concern is born out of the fact that Israeli intelligence has engaged in this exact type of behavior before as part of the PROMIS software scandal, whereby Israeli "superspy" Robert Maxwell sold bugged software to the U.S. government, including highly sensitive locations involved in classified nuclear weapons research. When that software, known as PROMIS, was installed on U.S. government computers, Israeli intelligence gained access to those same systems and devices.

The U.S. government was not the only target of this operation, however, as the bugged PROMIS software was placed on the networks of several intelligence agencies around the world as well as powerful corporations and several large banks. Israeli intelligence gained access to all of their systems until the compromised nature of the software was made public. However, Israel's government was not held accountable by the U.S. government or the international community for its far-reaching espionage program, a program directly facilitated by technology-focused front companies. The similarities between the products marketed and clients targeted by Maxwell during the PROMIS scandal and currently by Toka are considerable.

World Bank, IDB aid Toka in targeting Palestine's allies

While the ties between Toka and Israel's national security state are clear as day, what is also significant and unsettling about this company is how its entry into developing and developed countries alike is being facilitated by global financial institutions, specifically the World Bank and the Inter-American Development Bank. Notably, these are the only deals with governments that Toka advertises on its website, as the others are not made public.

Several projects funded by one or another of these two institutions have seen Toka become the "cyber designer" of national cybersecurity strategies for Nigeria and Chile since last year. Significantly, both countries' populations show strong support for Palestine and the BDS movement. In addition, Toka garnered a World Bank-funded contract with the government of Moldova, an ally of Israel, last September.

The World Bank selected Toka in February of last year to "enhance Nigeria's cyber development," which includes developing "national frameworks, technical capabilities and enhancement of skills." Through the World Bank contract, Toka has now become intimately involved with both the public and private sectors of Nigeria that it relates to the country's "cyber ecosystem." The World Bank's decision to choose Toka is likely the result of a partnership forged in 2019 by the state of Israel with the global financial institution "to boost cybersecurity in the developing world," with a focus on Africa and Asia.

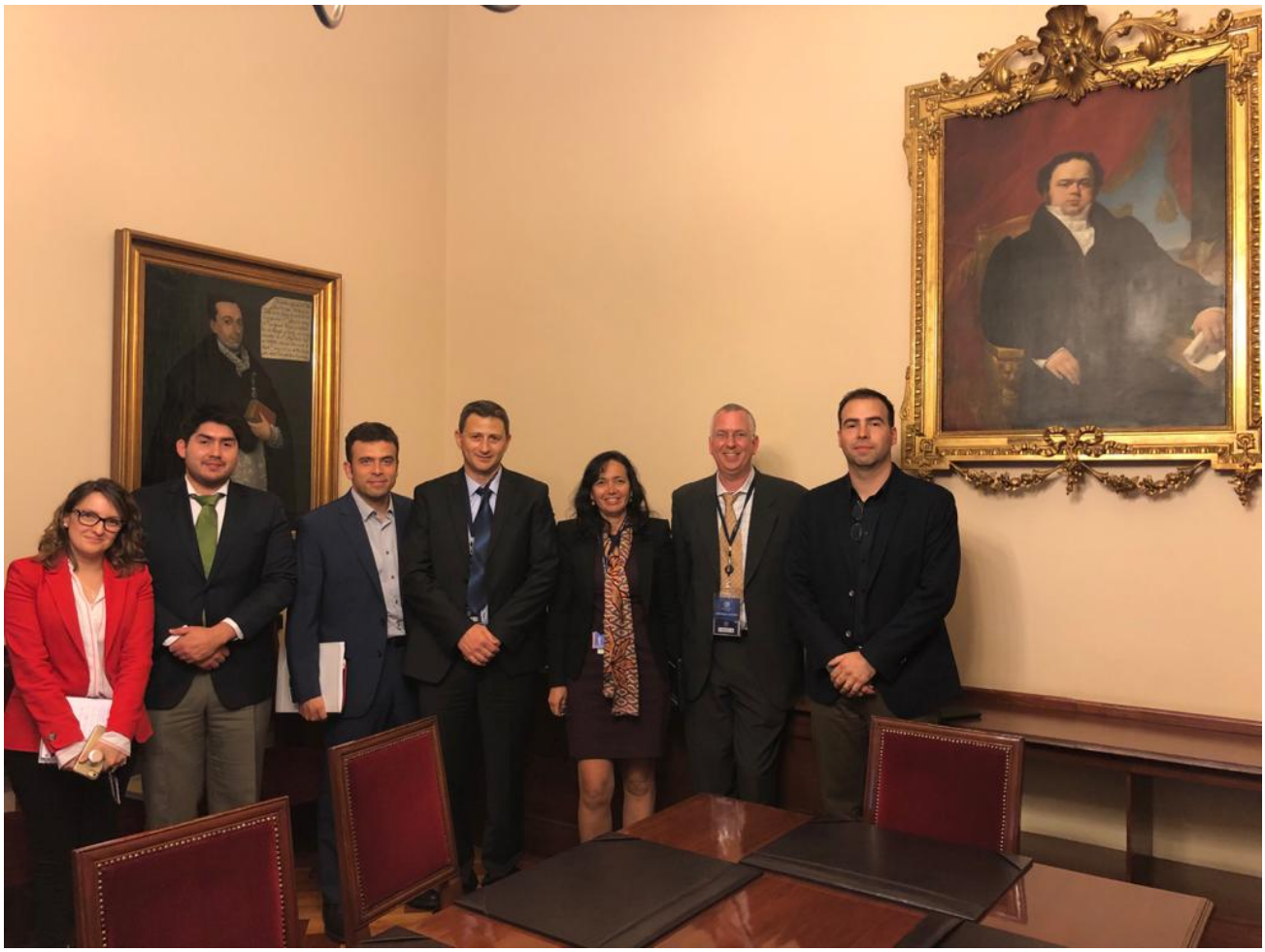
Toka executives pose with Nigerian officials in 2020. Photo | Israel Defense

“Designing and building sustainable and robust national cyber strategy and cyber resilience is a critical enabler to fulfilling the objectives of Nigeria’s national cybersecurity policy and strategic framework,” Toka CEO Yaron Rosen said in a press release regarding the contract.

Given Toka’s aforementioned use of its technology for only “trusted” governments, it is notable that Nigeria has been a strong ally of Palestine for most of the past decade, save for one abstention at a crucial UN vote in 2014. In addition to the government, numerous student groups, human rights organizations, and Islamic organizations in the country are outspoken in their support for Palestine. With Toka’s efforts to offer its products only to countries who align themselves with “friendly” countries, their now intimate involvement with Nigeria’s cyber development could soon have consequences for a government that has tended to support the Palestinian cause. This is even more likely given Toka CEO Rosen’s statements at an April 2021 event hosted by Israel’s Ministry of Economy, where he emphasized the role of cyber in developing countries specifically in terms of their national defense and economic strategy.

Three months after the deal was struck with Nigeria through the World Bank, the Inter-American Development Bank (IDB) selected Toka to advise the government of Chile on "next steps for the country's national cybersecurity readiness and operational capacity building." As part of the project, "Toka will assess the current cybersecurity gaps and challenges in Chile and support the IDB project implementation by recommending specific cybersecurity readiness improvements," per a press release. Toka claims it will help "establish Chile as a cybersecurity leader in South America." Regarding the deal, Toka's Rosen stated that he was "thankful" that the IDB had "provided us with this opportunity to work with the Government of Chile."

Israel signed consequential agreements for cooperation with the IDB in 2015, before further deepening those ties in 2019 by partnering with the IDB to invest $250 million from Israeli institutions in Latin America specifically.



Toka executives are pictured with Chilean officials during a 2020 meeting in Santiago

Like Nigeria, Chile has a strong connection with Palestine and is often a target of Israeli government influence efforts. Though the current far-right government of Sebastián Piñera has grown close to Israel, Chile is home to the largest Palestinian exile community in the world outside of the Middle East. As a result, Chile has one of the strongest BDS movements in the Americas, with cities declaring a non-violent boycott of Israel until the Piñera administration stepped in to claim that such boycotts can only be implemented at the federal level. Palestinian Chileans have strong influence on Chilean politics, with a recent, popular presidential candidate, Daniel Jadue, being the son of Palestinian immigrants to Chile. Earlier this year, in June, Chile's congress drafted a bill to boycott goods, services and products from illegal Israeli settlements.

While Toka frames both of these projects as aimed at helping the cyber readiness and economies of the countries it now services, Israeli media has painted a different picture. For instance, *Haaretz* wrote that Israel's partnerships with development banks, specifically those made in 2019 that resulted in these Toka contracts, were planned by an inter-ministerial committee set up by then-Prime Minister Benjamin Netanyahu "to realize the potential of international development to strengthen the Israeli economy, improve Israel's political standing and strengthen its international role." One source, quoted by *Haaretz* as being close to this undertaking, stated that "development banks are a way to help advance Israel's interests and agenda in the developing world, including Latin America. But it's not philanthropy."

Given these statements, and Toka's own *modus operandi* as a company and its background, it seems highly likely that the reason both Nigeria and Chile were chosen as the first of Toka's development banks contracts was aimed at advancing the Israeli government's agenda in those specific countries, one that seeks to counter and mitigate the vocal support for Palestine among those countries' inhabitants.

The spyware problem goes far beyond NSO Group

The NSO Group and its Pegasus software is clearly a major scandal that deserves scrutiny. However, the treatment of the incident by the media has largely absolved the Israeli government of any role in that affair, despite the fact that the NSO Group's sales of Pegasus to foreign governments has been approved and defended by Israel's government. This, of course, means that Israel's government has obvious responsibility in the whole scandal as well.

In addition, the myopic focus on the NSO Group when it comes to mainstream media reporting on Israeli private spyware and the threats it poses means that other companies, like Toka, go uninvestigated, even if their products present an even greater potential for abuse and illegal surveillance than those currently marketed and sold by the NSO Group.

Given the longstanding history of Israeli intelligence's use of technology firms for international surveillance and espionage, as well as its admitted policy of using tech companies as fronts to combat BDS and ensure Israel's "cyber dominance," the investigation into Israeli spyware cannot stop just with NSO Group. However, not stopping there risks directly challenging the Israeli state, particularly in Toka's case, and this is something that mainstream media outlets tend to avoid. This is due to a mix of factors, but the fact that NSO's Pegasus has been used to spy on journalists so extensively certainly doesn't help the matter.

Yet, Israel's weaponization of its tech industry, and the global use of its spyware offerings by governments and security agencies around the world, must be addressed, especially because it has been explicitly weaponized to prevent non-violent boycotts of Israel's occupation of Palestine, including those solely based on humanitarian grounds or out of respect for international laws that Israel routinely breaks. Allowing a government to engage in this activity on a global scale to stifle criticism of flagrantly illegal policies and war crimes cannot continue and this should be the case for any government, not just Israel.

If the outlets eagerly reporting on the latest Pegasus revelations are truly concerned with the abuse of spyware by governments and intelligence agencies around the world, they should also give attention to Toka, as it is actively arming these same institutions with weapons far worse than any NSO Group product.

Feature photo | Graphic by Antonio Cabrera

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 MintPress News. She currently writes for her own outlet Unlimited Hangout and contributes to The Last American Vagabond and MintPress News.