Pegasus: The Story of the World's Most Dangerous Spyware

Laurent Richard and Sandrine Rigaud
London: Macmillan, 2023, 317 pages

Colin Challen

This is the first book about Pegasus, the cyber surveillance software developed by the Israeli company the NSO Group. It lays out the threat posed by the world's leading cyber surveillance outfit. It is a sobering story, albeit told in a style which demands a film script, with its heroes (the authors) sacrificing their safety in pursuit of the truth – and, as journalists, keeping a lid on their story until their exclusive could be launched with all due credits rolling. In that context, the story revealed here is as much about them and their co-investigators as it is about Pegasus. Told in the first person, their book has the style of a thriller, and perhaps this explains why it has an index but no references.

Pegasus became much sought after by governments for its ability not only to take over your mobile phone (or laptop, tablet etc.) and listen in to your conversations, but also to take over the phone's other capabilities without you knowing it, and without leaving much of a trace. The *Financial Times* reported:

> The Israeli company whose spyware hacked WhatsApp has told buyers its technology can surreptitiously scrape all of an individual's data from the servers of Apple, Google, Facebook, Amazon and Microsoft, according to people familiar with its sales pitch.
>
> NSO Group's flagship smartphone malware, nicknamed Pegasus, has for years been used by spy agencies and governments to harvest data from targeted individuals' smartphones.
>
> But it has now evolved to capture the much greater trove of information stored beyond the phone in the cloud, such as a full history of a target's location data, archived messages or photos, according to people who shared documents with the *Financial Times* and described a recent product demonstration.

> The documents raise difficult questions for Silicon Valley's technology giants, which are trusted by billions of users to keep critical personal information, corporate secrets and medical records safe from potential hackers. [1]

Pegasus became widely controversial when a leak of 50,000 Pegasus-tapped mobile numbers – including the private numbers of leading politicians, such as French President Macron – was passed to the authors. The task then, with help from numerous assistants, was to identify who owned some of the leaked phone numbers. In many cases they had to ask presumed Pegasus victims to hand over their phones for forensic analysis, whilst not revealing their source and at the same time not alerting NSO to their digging. The original clandestine activity had to be met with similarly clandestine activity. At all times the authors had to take strict counter-surveillance measures to prevent NSO learning of and subverting their endeavours.

I don't for a moment deny that the authors have performed a valuable public service in further exposing the nefarious ways of cyber surveillance; and after theirs and other Pegasus revelations NSO took some heavy blows. What is missing from their account, however, is much of the context – chiefly, how and why did an Israeli company become a world leader in cyber surveillance? There are clues in the book, and these extracts are worth quoting at length.

> Whatever the talk among the world of [Israeli Defence Force Unit] 8200, Shalev and Omri [NSO's founders] and the rest of NSO must have taken heart in the support they got from the Israeli officialdom, like when Citizen Lab produced a series of reports toward the end of 2017 about the abuses of Pegasus technology in Mexico. Researchers in Toronto had documented Pegasus spyware attacks against about twenty people there, including reporters, human rights lawyers, opposition politicians, and even the outspoken parents of one of the student-teachers taken off the bus and murdered by a drug cartel in Ayotzinapa. When Shalev and Omri refused to speak to any specific charges but suggested instead a nefarious anti-Semitic plot afoot within Citizen Lab, Israeli government apparatchiks joined the chorus singing cabal and conspiracy. "I can tell you that's for sure that we see the fingerprints and footprints of anti-Israel and even anti-Semitic

[1] *Financial Times* 19 July 2019 <https://www.ft.com/content/95b91412-a946-11e9-b6ee-3cdf3174eb89>

> elements [at Citizen Lab]" says one of Netanyahu's key advisors from the time, without adducing a whit of evidence.
>
> The Citizen Lab reports did prompt a legal petition in Israel to forbid the sales of Pegasus to governments that regularly violated human rights, but the petition was waved away. The Supreme Court in Israel refused to interfere with MOD decision-making, or to air the suit in public, or to even release the full text of the judgement to the public. The judges agreed with the Netanyahu government that the details of the cyberweapons license needed to be kept under seal. "Our economy, as it happens, rests not a little on that export," Supreme Court President Justice Esther Hayut had once said. (pp. 194/195)
>
> [. . . .]
>
> Netanyahu's government lacked easy and open channels to spread [diplomatic] incentives in the capital cities of Rabat, Riyadh, and Abu Dhabi. No embassies, no consulates, no foreign service officers on the ground. Israel's chief point contact with these wary allies was its international intelligence service, the Mossad. "Mossad is in charge of building diplomatic connections with the regimes where we don't have a diplomatic relationship," one former Israeli intelligence commander explained to us. When their intelligence counterparts in these countries started asking for Unit 8200-level spyware technology to fight ISIS or homegrown terrorists, the Mossad had to demur. The Israeli military did not share its technology with anyone, not even close allies like the US and the UK. But Mossad could offer the next best thing, which was Pegasus. NSO's technology was top-self, and NSO could be trusted to keep their collective mouths shut about who was buying and operating its spyware system. (p. 247)

In this sense the likes of NSO and *inter alia* Pegasus can be seen as an extension of the Israeli state, a useful but distanced part, allowing for some degree of deniability. But how far does this deniability extend? Unit 8200 has a strong belief in its technological superiority, its core role in the defence of the state and inseparability with the numerous spin-offs it has spawned. A legitimate question is whether the cyberware exemplified by Pegasus has a 'back door' for state surveillance by the Israeli intelligence services – a facility much desired by governments which continuously seek to navigate around encryption protections to obtain data in the never-ending 'war on terror'.

The similarity between the activities of the private company NSO and those of Unit 8200 is illustrated by a Unit 8200 cyber development called ‘Flame,’ described thus:

> . . . state-sponsored cyber espionage malware that circumvented anti-virus programs and remained undetected between two and five years. Aimed to map Iran’s computer networks and monitor computers of Iranian officials, it was designed to provide intelligence to help in a cyber campaign against Iran’s nuclear program. It also infected computers in the West Bank, Sudan, Syria, Lebanon, Saudi Arabia and Egypt.
>
> Flame was capable of stealing data from infected computers, logging keystrokes, activating computer microphones to record conversations, and taking screenshots. What made it so effective was its ability to constantly evolve in order to send home intelligence to an unknown spy-master controlling servers around the world. Then, once it needed to be extracted, the virus could clean out the insides of the computer where it had been hiding, leaving behind no evidence that it had ever been activated. The data-mining operation involved the National Security Agency, the CIA and Israel’s military.[2]

One would be hard put to slide a cigarette paper between the above malware description and Pegasus’s capabilities, except perhaps for the final sentence. But it would be impossible to doubt that the likes of the NSA and CIA (and their foreign equivalents) don’t take an interest in the malware products of private companies, especially those with connections to Unit 8200. It was reported that the FBI had bought Pegasus in 2019 but that they hadn’t chosen to use it.[3] The same report said that the US government had blacklisted NSO for fear it could jeopardise national security. It is clearly the case that less well-resourced government security agencies have relied on Israeli cyber security products rather than develop their own – they may need to pay heed to the US decision. Why should this be the case? A publication produced by BICOM, a UK-Israeli lobbying organisation, boasted:

> In the cyber security field, Unit 8200, the signals intelligence unit of the IDF’s military intelligence division, is renowned for attracting among the best and brightest Israeli recruits. After three years of

[2] Jeff Halper, *War against the people* (London*:* PlutoPress, 2015), p. 107

[3] *New York Times*, 28 January 2022 <https://archive.md/3OcKR>>

> military service these individuals go to university or into industry with a wealth of hands on experience and strong personal network, *and often retain their links with 8200 through reserve duty*. This expertise is recognised internationally. Ben Brabyn, Chief Executive of the Level 39 technology hub told BICOM that "the Israeli brand is very strong and the legendary status of 8200 is pretty well known among expert consumers, which creates a strong appetite for Israeli cyber expertise".[4] (emphasis added)

Israeli military reserve duty can typically last decades with the real possibility of being activated at any time, as has been demonstrated by a call-up in April 2023 to meet a potential escalation in violence in the country. One is bound to ask whether being a military reservist and working in private cyber security leads to a potential conflict of interest? Or whether those interests are harmoniously aligned? With what has been deemed by the Israeli government as akin to an existential threat, the BDS (Boycott, Divestment and Sanctions) movement must certainly be seen as an enemy worthy of combined cyber-surveillance, by both public and private sector operations.

An example of this close alignment of interests is provided by a report, released by Wikileaks, which details the activities of a company named Hazard Threat Analysis Ltd. In a presentation, HTA's founder and CEO, former Israeli Defence Intelligence Lt.Col. Aviram Halevi said:

> [HTA's] researchers are often recently discharged members of Israeli Defense Intelligence's (IDI) elite Unit 8200, which is well known in Israel as IDI's signal intelligence unit. The young staff is employed by HTA to develop online identities (avatars) in discussion groups used by potential terrorists to actively solicit information useful to their clients. Some of these identities have been maintained for as long as two years. Halevi was quick to note that his employees are not involved in terrorist planning online, limiting themselves to observer status within the groups.[5]

[4] BICOM, *UK-Israel relations after Brexit: cyber security* (London, 2018) p. 6, available at <https://tinyurl.com/y6866bdx> or <http://www.bicom.org.uk/wp-content/uploads/2018/04/cyber-security-UK-Israel-relations-after-Brexit.pdf>.
I wonder who exactly this credit is owed to? The document ends with the statement: 'This report has been produced by BICOM's research team in consultation with British and Israeli cyber security experts. We are grateful for their help.'

[5] <https://wikileaks.org/plusd/cables/08TELAVIV592_a.html>

HTA's sister company in the UK was called Hazard Management Solutions Ltd, but it was dissolved in 2018. Nevertheless, a mention of it on Bloomberg gave a flavour of the private/public integration of its services:

> The Company supplies integrated counter improvised explosive device training, analysis, and consulting services. HMS, through its United States and United Kingdom offices, offers its services to governments, armed forces, law enforcement, and commercial organizations worldwide.[6]

The NSO group took this integration to another level (literally) when they announced they had devised software called Eclipse which

> commandeers intruding drones and, according to NSO, costs "hundreds of thousands of dollars" to provide stadium-sized protection. More than 10 countries have bought it to safeguard sites like energy facilities, NSO said.[7]

At this point one might well ask, 'So what? Wasn't the private sector always enmeshed with government in the "military industrial complex?"' Yes, of course it was and is. In the UK one only needs to think of BAE Systems, the firm which mops up so much taxpayers' money. Whilst BAE has recruited retiring senior military personnel to their board, the company and its products have also literally replaced more lowly personnel in many areas. But I would argue the arena we are now moving into is categorically different, in terms of both technology and governance.

Technology first. We could make a comparison between analogue and digital warfare. Analogue warfare relied (and still does to a large extent) on blowing things up, destroying buildings and people. This mode of warfare still seems to predominate in the Ukraine conflict. In that particular case, if we look at the Russians' attempts to knock out Ukrainian infrastructure, bombs and missiles are still the order of the day. Perhaps that is because Russia, despite its alleged cyber capacity has not yet made a cyber weapon as successful as the Israeli/US Stuxnet malware which targeted Iran's nuclear installations – causing actual physical damage. Cyber warfare will, in time, become more prevalent now we are entering what has been called 'the internet of things'. Entire

[6] <https://tinyurl.com/38bedubm> or <https://www.bloomberg.com/profile/company/955021Z:LN?leadSource=uverify%20wall>

[7] <https://tinyurl.com/sb7sdyh9> or <https://www.middleeastmonitor.com/20200608-israels-nso-spyware-group-shows-off-anti-drone-tech/>

networks supporting health, transport, power and communications will become more vulnerable (which of course makes the cyber security companies even more necessary). This is the new arms race, and military preparedness is increasingly focussed on the threat. The danger here is of leakage – which is something that doesn't really happen with bombs and missiles. By this, I mean that the technology will be harder to contain, no longer kept in a bunker behind barbed wire. Thus, Pegasus represented a form of such leakage: an instance where malware was widely used in a way that wasn't originally intended.

On the issue of governance, one could argue that cyber weapons are far more secret, and likely to be more opaque than their predecessors. There will be no military parades touting the latest weapon. Because of the invisibility of malware it will be less accountable and, as we've seen with NSO, it will be given special treatment politically. Unlike a missile, this is an area of production which is continually evolving, whose current status for obvious reasons must always be kept under wraps. It forms part of an ongoing battle between states and non-state actors. Indeed, cyber weapons seem to be used indiscriminately between allies and enemies. Because of the complex and advanced nature of the technology involved, I doubt that lay-person legislators will ever really understand – and thus they won't really know – what's going on under their noses. To deflect criticism, the response of NSO was to mount what might be described as an 'ethics washing' defence, creating an 'advisory' board of ex-politicians and others who could be wheeled out as champions of responsibility as the need arose. One of NSO's advisory board members, for example, was Tom Ridge, the first U.S. Secretary of State for Homeland Security and Republican Governor of Pennsylvania 1995-2001.[8]

By way of an aside, it amuses me that cyber-security businesses feel compelled to publish details of their Director and Advisory Board members prominently on the web. Pride perhaps dictates that they should show off their credibility in finance, politics and intelligence, but if they have their finger on the button, why should they need to advertise? Don't they know who their customers are, even before their customers do? Perhaps there's some real competition in this business – which contrasts with state intelligence apparatus, where at least amongst friendly countries co-operation might be seen to be advantageous. I have noted

[8] <https://www.reuters.com/article/cyber-rights-nso-idINL5N2602JM>

before how some of these advisory boards are peopled.[9]

Israel's cyber investment has been an economic boon as well as a strategic success. Pegasus may have helped pave the way down the diplomatic road towards some reconciliation with some Middle Eastern neighbours (in the process further isolating the Palestinians, another strategic goal). And, as noted earlier, cyber technology has benefitted Israel's economy disproportionately – on a per capita basis Israel is possibly the world's largest exporter of cyber technology. The big question remains: how much, if any, of this technology has a back door? Has the insatiable thirst for intel – on friend and foe alike – been catered for?

Colin Challen is a former Labour MP
and blogs at www.colinchallen.org.

[9] 'Peer Group Pressure', in *Lobster* 78 at <https://tinyurl.com/2czsykja> or <https://www.lobster-magazine.co.uk/article/issue/78/peer-group-pressure/>.