Seeing the world like a Palestinian

Intersectional struggles against Big Tech and Israeli apartheid

Apoorva PG

STATE OF POWER 2023

tni
transnationalinstitute

In May 2021, as Israeli forces launched an intense wave of airstrikes on the besieged Gaza Strip—resulting in 256 Palestinian casualties and tens of thousands injured—Google and Amazon Web Services (AWS) signed Project Nimbus[1], a $1.2 billion contract to provide cloud services to the Israeli government and military. The two corporations would effectively provide the technological backbone of Israel's occupation of Palestinian territories. Three data centres are already underway for this project. Amazon Web Services also provided the cloud platform[2] for Pegasus spyware until the news on Pegasus Project broke, and continues to do so for the Blue Wolf app,[3] which allows Israeli soldiers to capture images of Palestinians across the occupied West Bank and then matches them with military and intelligence databases.

With its far-reaching and unprecedented impact, the contract is just one manifestation of the profound links between Israel and Big Tech corporations. Hewlett Packard Enterprise (HPE), for example, had an exclusive contract to provide servers from 2017 to 2020 for Israel's population database[4], which was also used to determine various forms of exclusion of Palestinian citizens of Israel and residents of occupied East Jerusalem. Big Tech has helped sustain an occupation built on military control and perpetual surveillance, which Palestinians have for decades denounced as a form of apartheid and as 'settler colonialism'.[5] Amnesty International[6] and other international organisations, the UN Special Rapporteur on human rights in the Occupied Palestinian Territories (OPT), and a growing number of governments believe that Israel is committing the crime of apartheid.

The ubiquity of digital technology and control, alongside the monetisation of personal data, have led to data becoming the new frontier of colonialism. Understanding the role of Big Tech in consolidating Israel's violation of Palestinian human rights brings into sharp relief the urgent need to challenge this global data colonialism. This is both because methods of repression tested on Palestinians are being adopted across the world, and because in questioning Big Tech, its collusion with military and surveillance agencies and its theft of our data enables us to build intersectional struggles against the *matrix of oppression*—of militarisation, neoliberal capitalism and Israeli apartheid—that Big Tech bolsters and from which it profiteers.

The deep ties between Israel and Big Tech have enabled a two-way flow of profit, crime and complicity. This enables Israel to deploy fast-innovating technology developed by transnational corporations (TNCs) and integrate it in its surveillance, control and repression of Palestinians. At the same time, Israeli technology developed to control the Palestinian people is made available for Israeli and international tech companies to scale up and export to other countries for repressive purposes. Consider some of these statistics compiled by Palestinian Stop the Wall campaign in its Digital Walls[7] report:

- During the last few decades, over 300 leading technological multinational corporations established R&D centers in Israel, accounting for about 50% of the business enterprise R&D [research and development] expenditure.
- These multinational corporations have acquired a total of 100 Israeli companies. A number of them, such as—Intel, Microsoft, Broadcom, Cisco, IBM and EMC—acquired over ten local companies over the span of their operation in Israel.
- More than 30 tech Unicorns—start-up companies valued more than 1 billion US$—are located in Israel. This is around 10% of the world's unicorns.

This symbiotic relationship drives Big Tech's investment in Israel, and reinforces the growth of militarised digital technology and surveillance, which has been pioneered by but is not unique to Israel.

Big Tech and Global Imperial Wars

The specific context of Big Tech and apartheid Israel is part of a global power structure of domination, racism and coercive states. Digital technology includes surveillance systems first used by the military, as the Digital Walls report argues[8]:

> Both processes—the digitalization and the militarization—are not only partially time wise parallel developments. They are deeply intertwined: the first computers emerged from World War II and the internet was developed in the Cold War by the US military. No wonder that military technology, research and industry is gaining huge profits from the start of the digital economy.

The Pentagon's Project Maven illustrates how these processes and their interlinkages continue to grow in tandem with global, imperial wars. Since early 2000, the US military has used drones to attack targets in other countries, also causing civilian casualties.[9] Project Maven is geared to further drone attacks by analysing surveillance footage with the use of Artificial Intelligence (AI). Google was initially contracted for this project, but withdrew in the wake of objections by its own employees. The contract then went to AWS and Microsoft,[10] and has since been transferred to the US National Geospatial-Intelligence Agency (NGA).[11]

The Big Tech Sells War[12] project, which has been tracking the collusion between US tech corporations and anti-Muslim violence and Islamophobia, noted that '(t)he [Patriot] act authorizes sweeping powers for the government to surveil Americans and even indefinitely detain immigrants who aren't charged with crimes. Its passage opened the doors for Big Tech to become, first and foremost, the brokers of our personal data, selling to government agencies and private companies at home and abroad and unleashing the era of the data economy'. The US National Security Agency (NSA), whose mass surveillance programme was exposed by the former contractor and whistle-blower Edward Snowden, had access to Microsoft servers in September 2007; to Google in January 2009; to Facebook in June 2009; to YouTube in 2010; and to Apple in October 2012, mandated by amendments to Foreign Intelligence Surveillance Act, which have since been renewed.

Decades of normalising mass surveillance, the introduction of remote drone attacks by the US military, and building walls and other border-control mechanisms to prevent the entry of immigrants, have depended on constantly advancing technology to classify, surveil and attack people. This runs parallel to Big Tech becoming the multi-billion-dollar industry that it is today. A timeline of both trajectories[13]—of evolving technologies of repression and the growth of Big Tech—can be found in the Big Tech Sells War campaign. In 2013, AWS won its first cloud contract[14] in the US with the CIA, the National Security Agency (NSA) and other US intelligence agencies. In April 2022, the NSA re-awarded[15] a (separate) $10 billion contract for cloud-based computing services to AWS. Microsoft protested against AWS winning this contract, the successor of the Joint Enterprise Defense Infrastructure (JEDI) IT contract, which Microsoft had in 2019. In March 2021, Microsoft signed up to provide HoloLens augmented-reality headsets to the US military[16] in a contract worth about $21.88 billion over 10 years.

Big Tech Sells War calculates that over the last 20 years, Big Tech contracts with the Pentagon and Department of Homeland Security (DHS) have amounted to approximately $44 billion. It also exposes the (unsurprising) revolving door between the US defence establishment and Big Tech executives: at the time of writing, the Director of Security at AWS, Steve Pandelides, had worked for the Federal Bureau of Investigation (FBI) for over 20 years, including at the National Counterterrorism Center and Operational Technology Division. Jared Cohen worked at Google where he founded Jigsaw, tasked with developing counter-terrorism tools for social media platforms among other things. He was previously Policy Planning Staff for the US State Department and now works at Goldman Sachs.

In many ways, Big Tech builds on the military-industrial complex model in creating a new tech-military complex. But unlike the brazen nature of the traditional arms-production industry, where weapons are obviously designed to kill and repress, Big Tech is more insidious because it simultaneously claims to be democratic and accessible. The blurred distinction between military and civilian use helps normalise its ubiquity and dulls our response to the urgent challenges it presents.

Israel's Apartheid Technology

Seeing the situation from the Palestinians' perspective helps clear the fog, given the complicity of Big Tech in Israel's apartheid system. Since before its establishment in 1948, through the ethnic cleansing of hundreds of thousands of Palestinians, Israel has deployed its military and surveillance apparatus to further dispossess, fragment and disempower them. The Intelligence Corps of the Israeli Occupation Forces, Unit 8200, was founded in 1952. Since then it has been tasked with collecting intelligence and decrypting code. Spying and mass surveillance of Palestinians is the driving force behind much of Israel's rapid development of new technologies. Here is how Israel's Innovation Authority talks about cyberwarfare[17]:

> Cyberwarfare has always been at the forefront of the Israeli high-tech industry. [...] The winning combination of graduates from IDF [Israel Defense Forces] technology units and an innovation environment supported by the Innovation Authority enables cutting-edge Israeli technology to shape the future starting today.

Israel exports this security paradigm—of manufactured fears justifying responses by authoritarian responses by states to ensure their 'security' and 'survival', along with its weapons and technologies. In the case of Israel's apartheid regime, this need for security extends only to the Jewish population while Palestinians live in varying degrees of disenfranchisement, stripped of security by Israel's policies.

Unit 8200 can tap any phone conversation in the Occupied Palestinian Territories. There are facial-recognition cameras installed—one for every 100 Palestinians—in occupied East Jerusalem. Private information is used to blackmail Palestinians[18] into becoming informants. Hawk Eye cameras designed to read license plates allow the Israeli police forces to obtain information and the location of vehicles in real time. Israeli checkpoints have facial-recognition technology installed, initially provided by HP. The 'Blue Wolf' app, dubbed the Israeli army's secret 'Facebook for Palestinians', captures images of Palestinians all over the occupied West Bank and matches them with the database run by Israeli military and intelligence. Israeli soldiers are rewarded for capturing[19] a large number of photographs of Palestinians under occupation.

Not even Jeremy Bentham's 'panopticon' captures this situation as it aimed only to *watch in order to control,* whereas Israel and its tech apparatus aims to *watch, coerce, blackmail and violate*—all within the framework of its apartheid regime.

Just like the arms industry, Israel's digital technology sphere is deployed within an apartheid system, whereby tools and applications are 'field-tested' on Palestinians before they are exported. Jalal Abukhater, in the article cited earlier, notes:

> For Israeli companies engaged in developing the surveillance and spyware technologies, the occupied territories are just a lab where their products can be tried before being marketed and exported worldwide for profit. For the Israeli government, this surveillance regime is both a tool of control and a money-making business.

Indeed, as the Pegasus Project revealed, the Israeli NSO Group's Pegasus spyware has been used across the world to spy on journalists and activists as well as government and opposition leaders. In India, for example, the list of those targeted by Pegasus spyware includes anyone articulating a serious challenge to Modi's right-wing government. That Israeli weapons and military technologies are used as a means of repression worldwide is well known. Still shrouded, however, is the role of Big Tech in Israel's production and export of repressive technologies.

Big Tech Profits from Apartheid

While its apartheid and settler colonial regime is the 'lab' for producing repressive weapons[20] and technology, it is Big Tech which provides the necessary investment and supports the proliferation of Israel's IT and cyber-security industry, from which it richly profits.

Major tech giants, from Microsoft to Google to AWS are actively engaged in Israel's tech industry. Microsoft reportedly acquired two Israeli cyber-security companies between 2015[21] and 2017[22]. Adallom, which was founded by a veteran[23] of the Israeli Intelligence special unit, was bought in 2015 for $320 million in 2015, and Hexadite for $100 million in 2017.

In 2019, AWS, contracted along with Google to build Israel's cloud platform along with Google, worked with local data centres to set up the cloud infrastructure. As part of the Nimbus project, Google has recently set up a local cloud region in Israel. According to the contract the two companies have 'committed to making reciprocal purchases and launching industrial cooperation[24] in Israel equivalent to 20% of the value of the contract'. Facebook's second largest R&D centre is also based in Israel.

States which buy Israeli spyware and digital technology to repress their citizens are entrenching Israel's apartheid regime and need to be challenged, along with exposing the complicity and profiteering by US-based Big Tech corporations.

Praxis of Intersectionality: The No Tech for Apartheid campaign

Big Tech's expanding control and complicity in military repression have been countered by diverse challenges and grassroots resistance. From the early phase of whistle-blowers' exposés to current campaigns exposing Big Tech's profiteering from war, there is a growing demand to end the weaponisation of technology.

In the US, for example, a grassroots-based No Tech for ICE[25] campaign highlights the key role played by Palantir and AWS in providing the infrastructure for Immigration and Customs Enforcement (ICE) along with other law-enforcement agencies involved in the Trump administration's brutal family-separation policy. Palantir gathered information on individuals, which enabled state agencies to track and build profiles of immigrants to be deported, while AWS provided servers to host Palantir's tools.

Community organisers are fast recognising and responding to the digital mode of militarisation and repression, seen not only in the tech giants' exports to repressive states but also in how digital censorship and silencing are used to crush the voices of resistance and amplify right-wing, regressive ideologies. This has also been highlighted by digital rights groups such as 7amleh, the Arab Center for Social Media Development, and Sada Social, which have shown how during the 2021 Gaza assault and in the ensuing popular struggle, Palestine-related content was censored[26] by social media platforms such as Facebook and Instagram. There is a growing discourse of digital rights which brings together grassroots organisers and tech experts who are working to make the digital sphere open and democratic rather than serving as a tool for subjugation.

Joining these forces are various current (and former) tech company employees, striking against their products being used to violate the rights of marginalised people, and for military purposes. They highlighted the profound ethical implications of any involvement in the automation of warfare. In 2018, a year before it was due to expire, Google announced that it would not be renewing[27] its contract with Project Maven. As stated earlier, Microsoft and AWS won the contract.

The campaign against Project Nimbus presents a crucial opportunity to bring together the struggles against Big Tech from various perspectives—Palestinians and solidarity activists, tech workers, digital rights, and labour and anti-militarisation activists.

Months after the contract was announced, 90 Google and 300 Amazon employees wrote an open letter condemning it and opposing their employers' decision to 'supply the Israeli military and government technology that is used to harm Palestinians'. Some of the protestors faced retaliation, such as Ariel Koren, who was given an ultimatum to relocate from the US to Brazil, despite large public petitions against this action. Koren left Google in August 2022, noting in her resignation statement that, 'Google systematically silences Palestinian, Jewish, Arab and Muslim voices concerned about Google's complicity in violations of Palestinian human rights—to the point of formally retaliating against workers and creating an environment of fear'. Others joined her in speaking out against the retaliatory action taken against those who supported this campaign.

Along with the deep complicity of AWS in Israel's IT and cybersecurity industry, and its support for repression elsewhere as seen in the ICE example, its track record in the inhumane treatment of workers and union busting[28] has been widely reported. The formation of the Amazon Labor Union on Staten Island was, therefore, a historic moment in the US labour movement. Taken together these employees' actions are likely to be causing some concern among today's Big Tech CEOs.

Beyond the support to military and surveillance agencies, in essence contributing to deepening militarisation of people's daily lives, there is also the question of Big Tech's control over our data. Aspects of our lives that leave traces in the virtual world—now all but inevitable—are woven into algorithms that profoundly influence our choices, political opinions and decisions. Digital rights movements call for the defence of our privacy and security and against the commercialisation of personal data, nowhere more evident than with Google. There is a growing challenge to the control of Big Tech over individual lives and choices codified into data. The alternatives to data colonialism have also prompted lively debates on open source, public ownership and so on.

At the sharp end of digital colonialism, Palestine is therefore a sign of what is to come—and hence the point where we must first resist. In the name of bridging the digital divide, Big Tech is becoming more deeply entrenched, extracting data and profiteering from it. The COVID-19 pandemic exacerbated this as people around the world had to work and study from home, mostly without access to digital technology and equipment.

The growing interest of students and academics in questioning the control of Big Tech companies, such as Google, in the field of education, and its direct link with the oppression of Palestinians, prompted the global No Tech for Apartheid campaign to develop a toolkit for organising on university campuses.

The campaign against Project Nimbus stands at the intersection of Palestinian solidarity and anti-apartheid, labour rights, digital rights, decolonial and demilitarisation movements. In this evolving movement, it offers a clear look at the *matrix of oppression* of militarisation, neoliberal capital Israeli apartheid—all of which Big Tech bolsters and from which it draws massive profits. It builds on the understanding developed by campaigns against Big Tech in war, and brings together many struggling communities against a contract which has deep implications for everyone. Interlinked systems that oppress us demand that our forms of resistance also unite, to defy the forces that seek to isolate us. Solidarity exists only in action, and through its very existence as an intersectional force it undermines the violence inflicted by colonialism, patriarchy, racism and neoliberalism. Technology is not designed to be neutral, and as aspects of our lives move further into this sphere, and its operations and mechanisms remain far from democratic, with the force of global resistance its basic tools can yet be made democratic and accessible.

BIOGRAPHY

Apoorva PG is Asia Pacific campaigns coordinator for the Palestinian Boycott, Divestment and Sanctions (BDS) National Committee. She is among the organizers of BDS campaigns against HP Enterprises and Project Nimbus- the Google and Amazon contract to provide cloud services to the Israeli government and military. She has studied Sociology and was earlier part of access to education, copyleft and free software campaigns in India.

Endnotes

1 Endnotes: Scheer, S. (2021). Israel signs cloud services deal with Amazon, Google. *Reuters*. [online] 24 May. Available at: https://www.reuters.com/technology/israel-signs-cloud-services-deal-with-amazon-google-2021-05-24/ [Accessed 20 Mar. 2023].

2 Fung, B. (2021). *Amazon Web Services disables cloud accounts linked to NSO Group | CNN Business*. [online] CNN. Available at: https://edition.cnn.com/2021/07/19/tech/amazon-nso-group-pegasus-cloud-accounts/index.html [Accessed 20 Mar. 2023].

3 Middle East Eye. (2021). *Meet Blue Wolf, the app Israel uses to spy on Palestinians in the occupied West Bank*. [online] Available at: https://www.middleeasteye.net/news/israel-whats-blue-wolf-app-soldiers-use-photograph-palestinians.

4 WhoProfits. (2021). *Hewlett Packard Enterprise (HPE)*. [online] Available at: https://www.whoprofits.org/company/hewlett-packard-enterprise-hpe/ [Accessed 20 Mar. 2023].

5 Investigate & Dismantle Apartheid. (2022). *Al Haq issues landmark report 'Israeli Apartheid: Tool of Zionist Settler-Colonialism'*. [online] Available at: https://antiapartheidmovement.net/updates/view/al-haq-issues-landmark-report-israeli-apartheid-tool-of-zionist-settler-colonialism/15 [Accessed 20 Mar. 2023].

6 Amnesty International. (2022). *Israel's apartheid against Palestinians*. [online] Amnesty International. Available at: https://www.amnesty.org/en/latest/campaigns/2022/02/israels-system-of-apartheid/.

7 Stop The Wall. (n.d.). *Digital Walls*. [online] Available at: https://stopthewall.org/digitalwalls/ [Accessed 20 Mar. 2023].

8 Stop The Wall. (n.d.). *Digital Walls*. [online] Available at: https://stopthewall.org/digitalwalls/#militarization [Accessed 20 Mar. 2023].

9 Khan, A. (2021). Hidden Pentagon Records Reveal Patterns of Failure in Deadly Airstrikes. *The New York Times*. [online] 18 Dec. Available at: https://www.nytimes.com/interactive/2021/12/18/us/airstrikes-pentagon-records-civilian-deaths.html.

10 Brewster, T. (2021). *Project Maven: Amazon And Microsoft Scored $50 Million In Pentagon Surveillance Contracts After Google Quit*. [online] Forbes. Available at: https://www.forbes.com/sites/thomasbrewster/2021/09/08/project-maven-amazon-and-microsoft-get-50-million-in-pentagon-drone-surveillance-contracts-after-google/?sh=549483dc6f1e [Accessed 20 Mar. 2023].

11 Strout, N. (2022). *Intelligence agency takes over Project Maven, the Pentagon's signature AI scheme*. [online] C4ISRNet. Available at: https://www.c4isrnet.com/intel-geoint/2022/04/27/intelligence-agency-takes-over-project-maven-the-pentagons-signature-ai-scheme/.

12 Big Tech Sells War. *Big Tech Sells War - How Big Tech Sells War on our Communities*. [online] Available at: https://bigtechsellswar.com/ [Accessed 20 Mar. 2023].

13 Big Tech Sells War. *Big Tech Sells War - How Big Tech Sells War on our Communities*. [online] Available at: https://bigtechsellswar.com/#timelines-home [Accessed 20 Mar. 2023].

14 Nextgov.com. (2021). *NSA Awards Secret $10 Billion Contract to Amazon*. [online] Available at: https://www.nextgov.com/it-modernization/2021/08/nsa-awards-secret-10-billion-contract-amazon/184390/.

15 www.theregister.com. (2022). *$10b US defense cloud contract re-awarded to AWS*. [online] Available at: https://www.theregister.com/2022/04/28/nsa_wands_aws/.

16 Novet, J. (2021). *Microsoft wins U.S. Army contract for augmented reality headsets, worth up to $21.9 billion over 10 years*. [online] CNBC. Available at: https://www.cnbc.com/2021/03/31/microsoft-wins-contract-to-make-modified-hololens-for-us-army.html.

17 Israel Innovation. *Attack is the Best Form of Defense*. [online] Available at: https://innovationisrael.org.il/en/reportchapter/attack-best-form-defense [Accessed 20 Mar. 2023].

18 Mondoweiss. (2014). *Israel surveils and blackmails gay Palestinians to make them informants*. [online] Available at: https://mondoweiss.net/2014/09/blackmails-palestinian-informants/ [Accessed 20 Mar. 2023].

19 Abukhater, J. (2022). *Under Israeli surveillance: Living in dystopia, in Palestine*. [online] www.aljazeera.com. Available at: https://www.aljazeera.com/opinions/2022/4/13/under-israeli-surveillance-living-in-dystopia-in-palestine.

20 Alys Samson Estapé. (2021). *Israel: the model coercive state* and why boycotting it is key to emancipation everywhere [online] Available at: https://longreads.tni.org/stateofpower/israel-the-model-coercive-state [Accessed 20 Mar. 2023].

21 VentureBeat. (2015). *Microsoft confirms it has acquired cloud security platform Adallom*. [online] Available at: https://venturebeat.com/business/microsoft-confirms-it-has-acquired-cloud-security-platform-adallom/ [Accessed 21 Mar. 2023].

22 Lunden, I. (2017). *Microsoft to buy Israeli security firm Hexadite, sources say for $100M*. [online] TechCrunch. Available at: https://techcrunch.com/2017/06/08/microsoft-confirms-its-acquired-hexadite-sources-say-for-100m/?guccounter=2 [Accessed 21 Mar. 2023].

23 Algemeiner, T. (2021). *Unit 81: The Elite Military Unit That Caused a Big Bang in the Israeli Tech Scene - Algemeiner.com*. [online] www.algemeiner.com. Available at: https://www.algemeiner.com/2021/01/08/unit-81-the-elite-military-unit-that-caused-a-big-bang-in-the-israeli-tech-scene/ [Accessed 21 Mar. 2023].

24 Scheer, S. (2022). Google activates Israel's first local cloud region. *Reuters*. [online] 20 Oct. Available at: https://www.reuters.com/technology/google-activates-israels-first-local-cloud-region-2022-10-20/ [Accessed 21 Mar. 2023].

25 notechforice.com. *About | #NoTechForICE*. [online] Available at: https://notechforice.com/about/ [Accessed 21 Mar. 2023].

26 7amleh, the Arab Center for Social Media Development (2021). *#Hashtag Palestine 2021*. [online] Available at: https://7amleh.org/storage/Hashtag%202021%20EN.pdf

27 Statt, N. (2018). *Google reportedly leaving Project Maven military AI program after 2019*. [online] The Verge. Available at: https://www.theverge.com/2018/6/1/17418406/google-maven-drone-imagery-ai-contract-expire.

28 Kantor, J., Weise, K. and Ashford, G. (2021). The Amazon That Customers Don't See. *The New York Times*. [online] 15 Jun. Available at: https://www.nytimes.com/interactive/2021/06/15/us/amazon-workers.html