MARYAM ABU DAQQA FELLOWSHIP PUBLICATION

DIGITAL DOMINATION

AI, Surveillance, and Digital Power in Palestine and Beyond



جامعة بيرزيت
BIRZEIT UNIVERSITY
معهد ابراهيم أبو لغد للدراسات الدولية
Ibrahim Abu-Lughod Institute of International Studies

حملة - المركز العربي لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for the Advancement of Social Media

7amleh - The Arab Center for the Advancement of Social Media

DIGITAL DOMINATION
AI, Surveillance, and Digital Power in Palestine and Beyond
Maryam Abu Daqqa Fellowship Publication

Fellowship Fellows
Islam Al-Khatib
Arees Bishara
Sarah Fathallah
Melody Sepahpour
Rawan Natsheh

Editorial and Academic Contributions
Introduction
Jalal Abukhater
Policy Manager at 7amleh
Basil Farraj
Director of Ibrahim Abu-Lughod institute of International Studies, Birzeit University
Fellowship Academic Mentor
Mtanes Shihadeh
Fellowship Coordinator
Jalal Abukhater

Translation
Mersal Media
Design
Nour Sadat

This version is licensed under the following International License:
Attribution-NonCommercial-NoDerivs 4.0 International

To view a copy of the license, please visit the following link:
https://creativecommons.org/licenses/by-nc-nd/4.0

ialiis@birzeit.edu info@7amleh.org
ialiis.birzeit.edu www.7amleh.org
UpScrolled

In Memory of Maryam Abu Daqqa

Palestinian journalist murdered by
Israel in Gaza on 25 August 2025



This publication is dedicated to the memory of Maryam Abu Daqqa, a Palestinian journalist murdered by Israel in Gaza on 25 August 2025, while carrying out her professional and moral duty to document the realities of Palestinian life under siege, occupation, and genocidal war. Her work reflected the courage, integrity, and commitment that have long characterized Palestinian journalism.

The naming of this fellowship is both a tribute to Maryam Abu Daqqa and a recognition to the hundreds of Palestinian journalists, media workers, writers, photographers, and storytellers murdered while documenting injustice, preserving collective memory, and ensuring that Palestinian experiences remain visible to the world. Their work ensured that Palestinian experiences, voices, and aspirations continue to be recorded and shared despite attempts at erasure, silencing, and destruction.

We honor their memory and reaffirm the importance of knowledge production, documentation, and truth-telling as essential components of our struggle for justice and human dignity.

Introduction 5
Jalal Abukhater & Basil Farraj

Militarized Industrial Policy and Israeli Surveillance Firms 11
Islam Al-Khatib

From Settler Colonialism and the Remote-Control Occupation 36
Arees Bishara

Captive Voices: Algorithmic Voice Surveillance in Palestine 61
Sarah Fathallah

State Disinformation and Public Diplomacy Through Google 108
Melody Sepahpour

Artificial Intelligence in Gaza's Humanitarian System 139
Rawan Yousef

INTRODUCTION

The publication of this book comes at a time marked by the intensification of violence globally, deepening militarization, and the normalization of wars across multiple locations in the world. In Palestine, Israel continues to deploy a settler-colonial regime characterized by extreme forms of violence and torture, extending the genocidal war against the Palestinian population—most acutely in the Gaza Strip—while maintaining a comprehensive regime of control over Palestinian life across historic Palestine. Israel's domination operates not only through military force and visible violent tactics, but also through legal, economic, and technological mechanisms that regulate movement, hinder access to resources, employ violence, and violently attacks political and social mobilizations.

Beyond Palestine, the reach of Israeli military violence and war making extends into Lebanon, where violations of sovereignty, occupation of territory, and recurrent military attacks have subjected the Lebanese people to ongoing violence, forced displacement, and continuous threats to their livelihoods. At the same time, the United States, in close alignment with Israel, has unleashed a brutal war and aggressive economic policies toward Iran, including a fortified sanctions regime, military attacks, and forms of economic siege that continue to impact the livelihood of the Iranian people, and extend uncertainty and violence beyond Iran. These aggressive and violent policies continue to intensify regional tensions despite the recently declared fragile ceasefire.

Yet, these global dynamics are not confined to our region. In the United States, conduct by the Immigration and Customs Enforcement (ICE) has increasingly been characterized as resembling that of a paramilitary force.[1] Through expansive detention systems, surveillance infrastructures, and deportations, entire communities—particularly migrants and racialized populations—are subjected to criminalization, racialization, and systemic violence. The infrastructures enabling such systems increasingly rely on the growing concentration of data, predictive technologies, and AI-driven analytics developed by powerful private technology firms. Questions surrounding data extraction, centralized digital power, and AI-assisted surveillance are therefore no longer isolated to Palestine or war zones, but define global concerns shaping governance, borders, policing, militarization, and public life.

In the United Kingdom, the increasing integration of companies such as Palantir into state institutions and public infrastructure, including through £600 million worth of public contracts related to healthcare, policing, and military systems, illustrates the global proliferation and normalization of these technologies far beyond explicitly militarized contexts.[2]

1 Erica De Bruin, "ICE not only looks and acts like a paramilitary force – it is one, and that makes it harder to curb," The Conversation, January 28, 2026, https://theconversation.com/ice-not-only-looks-and-acts-like-a-paramilitary-force-it-is-one-and-that-makes-it-harder-to-curb-274580.

2 Matt High, "Palantir Faces Backlash Over £600m UK Government Contracts", BusinessChief, April 30, 2026, https://businesschief.com/news/palantir-faces-backlash-over-600m-uk-government-contracts.

Taken together, these examples illustrate a broader global condition in which militarization and violence have become enduring features characterizing today's world, disproportionately impacting marginalized, occupied, and racialized populations. Yet, the contemporary moment is distinguished not only by the persistence of physical violence—manifested in war, occupation, annexation, and enclosure—but also by the rapid expansion of less visible, technologically mediated regimes of control and violence. Central to this transformation is the intensifying integration of artificial intelligence and digital systems into military and security infrastructures.

What emerges across these contexts is a shared and deeply consequential pattern: the weaponization of advanced technologies to enable new modalities of surveillance, targeting, killings, and control. Artificial intelligence systems are increasingly used to process vast quantities of data, categorize individuals and populations, predict behavior, and facilitate both direct and indirect forms of violence and surveillance. These technologies do not merely accompany military operations; they actively reshape how power is exercised in the public sphere, extending the reach of state, non-state and corporate actors into the most intimate dimensions of daily life.

Indeed, a recent report by Amnesty International, titled "Tech made by Palantir and Babel Street pose surveillance threats to pro-Palestine student protestors & migrants," documents how U.S. authorities deploy AI-powered surveillance tools to monitor and target migrants, "non-citizens," and those speaking out for Palestinian rights.[3] Technologies developed by companies such as Palantir Technologies and Babel Street attests to the large-scale aggregation and analysis of personal data, facilitating practices of profiling, tracking, and categorization of entire populations, and their subjugation to brutal use of violence, surveillance and deportation regimes. The expansion of these technologies into civilian and public governance sectors demonstrates how AI-powered systems are increasingly embedded into everyday governance structures, normalizing surveillance and data extraction as ordinary administrative practice.

The Israeli state has likewise integrated AI systems into the core of its military and population-control regimes. Beyond the facial recognition technologies used across occupied Palestine to control the movements of Palestinians, the Israeli authorities have intensified their recourse to AI powered technologies in unleashing its genocidal violence and surveillance mechanisms.[4] Major technology corporations—including Google and Amazon—have played a significant role in this process,[5] most notably through examples such as Project Nimbus,[6] which provides cloud computing infrastructure and machine learning capabilities to Israeli governmental and military bodies. In parallel, AI-driven targeting systems—such as Lavender,

3 Amnesty International, "USA/Global: Tech made by Palantir and Babel Street pose surveillance threats to pro-Palestine student protestors & migrants," Amnesty International, August 21, 2025, https://www.amnesty.org/en/latest/news/2025/08/usa-global-tech-made-by-palantir-and-babel-street-pose-surveillance-threats-to-pro-palestine-student-protestors-migrants/

4 Amber Rahman, "Explainer: The Role of AI in Israel's Genocidal Campaign Against Palestinians," The Institute for Palestine Studies, October 16, 2024, https://www.palestine-studies.org/en/node/1656285.

5 Marwa Fatafta, "AI for War: Big Tech Empowering Israel's Crimes and Occupation," Al-Shabaka: The Palestinian Policy Network, October 26, 2025, https://al-shabaka.org/briefs/ai-for-war-big-tech-empowering-israels-crimes-and-occupation/.

6 See, for example, Amber Rahman, "Explainer: The Role of AI in Israel's Genocidal Campaign Against Palestinians," The Institute for Palestine Studies, October 16, 2024, https://www.palestine-studies.org/en/node/1656285.

The Gospel, and Where's Daddy—have been used to accelerate surveillance mechanisms and military attacks on Palestinians and have aided the Israeli regime as it expands its genocidal war and surveillance against the Palestinian population across historic Palestine.

The incorporation of AI into warfare is also evident in the ongoing Russia-Ukraine war. There, the battlefield has become a testing ground for emerging technologies, including autonomous drones, AI-assisted reconnaissance systems, and robotic platforms designed for surveillance, mine clearance, and combat support.[7] These developments signal a broader shift toward increasingly automated forms of warfare where algorithmic processes are increasingly aiding and reconfiguring geographies of violence.

It is within this rapidly evolving and deeply interconnected landscape where AI-powered and surveillance technologies have taken a center stage, and actively continue to impact political and social landscapes, that this book makes its intervention. The book seeks to critically examine the entanglement of artificial intelligence, surveillance systems, and corporate power in shaping contemporary regimes of violence and control in Palestine and beyond. It approaches these issues not as isolated phenomena, but as components of a global architecture in which technological innovation is closely aligned with violence, militarization, genocide, and surveillance technologies.

This publication represents the culmination of the first cohort of fellowships organized by 7amleh – The Arab Center for the Advancement of Social Media and coordinated by Jalal Abukhater. Named in honor of Maryam Abu Daqqa, a Palestinian journalist martyred in Gaza in August 2025, the fellowship received nearly 140 applications, reflecting the urgency and relevance of the themes it sought to address and unpack. Following a rigorous selection process, five fellows were chosen and supported through sustained mentorship.

Notably, all selected fellows are women. This outcome reflects the strength, depth, and analytical rigor demonstrated in their work. Three of the fellows are Palestinian, each grounded in distinct yet interconnected political realities: Jerusalem, Haifa, and the Palestinian refugee context in Lebanon. The remaining two fellows contribute critical perspectives from Iran and Morocco, expanding the geographic and analytical scope of the book.

The publication is the result of a collaboration between 7amleh: The Arab Center for the Advancement of Social Media and the Ibrahim Abu Lughod Institute of International Studies at Birzeit University. Both institutions have played a leading role in examining the intersections of technology, power, and rights, particularly in relation to the Palestinian context. The Ibrahim Abu Lughod Institute of International Studies at Birzeit University has recently hosted two international conferences addressing the militarization of the contemporary world, including discussions on AI, surveillance technologies, and pathways for strengthening transnational solidarity. The Institute alongside Al-Shabaka: The Palestinian Policy Network are organizing an international conference on "South-South Solidarity and Resistance

7 Nils Adler, "What do Ukraine's robot soldiers mean for the future of warfare?" Al-Jazeera, May 1, 2026, https://www.aljazeera.com/news/2026/5/1/what-do-ukraines-robot-soldiers-mean-for-the-future-of-warfare.

to Imperialism," that will similarly touch on the global state of violence shaping our world, and strategies of resistance and confrontation from and beyond Palestine.

Similarly, over the past years, 7amleh has conducted extensive research, advocacy, documentation and monitoring related to Palestinian digital rights and the growing role of technology in systems of domination and violence. This included investigations into digital censorship and suppression of Palestinian speech online, surveillance technologies and spyware, discriminatory platform governance, telecommunications blackouts in Gaza, data extraction and privacy concerns, AI-assisted warfare, and the role of major tech companies in facilitating or enabling violations of Palestinian rights. 7amleh has sought to position Palestinian experiences as central to understanding the global trajectories of digital authoritarianism, militarized technologies, and platform power.

This includes 7amleh's recent report, **Monetizing Occupation: Meta's Financial Enablement of Settlement Activity and Violent Rhetoric Against Palestinians**.[8] This report investigates how Meta permits Israeli far-right pages and settler-affiliated accounts to generate revenue despite promoting violent rhetoric, illegal settlement expansion, and attacks against Palestinians in the West Bank. Other work by 7amleh has similarly examined the deployment of AI-powered targeting systems in Gaza, the role of cloud computing infrastructures in supporting Israeli military systems, and the increasing use of digital technologies to fragment, monitor, and dominate over Palestinian political and social life[9].

Within this broader context, the five papers in this volume engage a range of themes related to the weaponization and impact of tech giants, artificial intelligence, and data extraction as mechanisms of surveillance and control that extend beyond the technological sphere. They also highlight the ways in which AI powered technologies circulate and constitute part of a broader geo-political economy of control that shapes their circulations, mobility and internationalization.

The first paper in this book, "Militarized Industrial Policy and Israeli Surveillance Firms," by Islam Al-Khatib traces the Israeli regime's emergence as a global cyber power, highlighting the deeply integrated public-private ecosystem linking military and intelligence institutions with a robust surveillance technology sector. It also emphasizes how these technologies are tested on Palestinians before being refined for global export, highlighting the transnational aspect of these technologies and their circulation.

The second paper, "From Settler Colonialism and the Remote-Control Occupation: Tech-innovation, Neoliberal Zionism, and digital sumūd in times of genocide," by Arees Bishara discusses how the convergence of technological innovation and military strategy has reconfigured the Israeli occupation into a form of digital settler colonialism, particularly following October 7,

8 Ahmad Qadi, Monetizing Occupation: Meta's Financial Enablement of Settlement Activity and Violent Rhetoric Against Palestinians (7amleh- The Arab Center for the Advancement of Social Media, 2026).

9 7amleh – The Arab Center for the Advancement of Social Media, "Palestinian Digital Rights, Genocide, and Big Tech Accountability," September 2024, https://7amleh.org/storage/genocide/English%20new%20(1).pdf

2023. It argues that Israel's innovation economy operates as both a national project and a global business model, embedding the technology sector within ongoing systems of violence.

The third paper, "Captive Voices: Algorithmic Voice Surveillance in Palestine," by Sarah Fathallah analyzes how voice has been weaponized into a highly sophisticated system of mass surveillance, transforming the act of speaking into an act of capture. It demonstrates how Palestinian voices are intercepted, algorithmically analyzed, and incorporated into systems of control that treat everyday expression as potential evidence or justification. The paper exposes the architecture of algorithmic voice surveillance in Palestine, revealing how speech itself has been transformed into a tool of domination.

The fourth paper, "State Disinformation and Public Diplomacy Through Google," by Melody Sepahpour examines the use of Google advertising as a tool of state-linked information influence, analyzing a year-long corpus of advertisements attributed to the Israeli government. It argues that Google Ads function as a powerful infrastructure for strategic communication, enabling state actors to insert preferred narratives at moments when users actively seek information, and how it had facilitated the Israeli regime's propaganda machine.

Finally, Rawan Yousef's "Artificial Intelligence in Gaza's Humanitarian System" explores the use of artificial intelligence and digital systems in humanitarian work in Gaza under conditions of siege, infrastructural devastation, surveillance, and external control. It examines how humanitarian staff engage with and navigate these systems in their daily work, showing that AI appears in two interconnected forms. The first in informal use of generative tools to manage administrative burdens, and the second in institutional systems that structure processes such as registration, verification, eligibility, reporting, and the circulation of humanitarian data.

Taken together, the contributions present in this book, highlight the urgency of analyzing the role of AI and tech companies in altering social and political realities, and renewing modes of coercion and violence worldwide.

Jalal Abukhater

Basil Farraj



Basil Farraj is the director of the Ibrahim Abu-Lughod Institute of International Studies and Faculty member in Philosophy and Cultural Studies at Birzeit University. His research focuses on political prisoners, carceral violence, and prisoners' confrontation practices against carceral regimes. His work also investigates the circulation of practices and policies across carceral regimes.



Jalal Abukhater is the Policy Manager at 7amleh - The Arab Center for the Advancement of Social Media. His work focuses on Palestinian digital rights, technology and human rights, corporate accountability, surveillance, artificial intelligence, and the intersections between digital infrastructures and systems of domination and violence.

ACADEMIC MENTORSHIP

Mtanes Shihadeh served as Academic Mentor for the first cohort of the Maryam Abu Daqqa Fellowship, accompanying the fellows throughout the research and review process.



He is a Palestinian scholar specializing in political economy, political behavior, and the relationship between economy and society in Israel/Palestine. He holds a PhD in Political Science from the Hebrew University of Jerusalem and an MA from the University of Haifa. His research focuses on Israeli economic and social policies, the political economy affecting the Palestinian community, and the impact of globalization on political and party structures. Palestinian scholar Mtanes Shehade serves as Director of the Israel Studies Program at Mada al-Carmel - The Arab Center for Applied Social Research in Haifa, and teaches in the MA Program in Israel Studies at Birzeit University.

MILITARIZED INDUSTRIAL POLICY AND ISRAELI SURVEILLANCE FIRMS

ISLAM AL-KHATIB

Introduction	12
Concepctual Framework	16
Methodology	19
Key Takeaways	33



Islam is a PhD candidate in Social Research Methods at the London School of Economics and Political Science. Born and raised in Lebanon, Islam is a Palestinian refugee researcher whose work centers on anti-colonial knowledge production. Her research connects surveillance, global technology infrastructures, and systems of domination.

Islam's research examines how Israeli surveillance technologies are integrated into global tech supply chains. Using investigative mapping, she traces how tools developed for occupation are rebranded and embedded in global governance systems as "public safety" or "cyber-security" infrastructures.

INTRODUCTION

Israel's position as a global cyber power is the outcome of a tightly integrated public-private apparatus, linking the military and intelligence establishment with a robust surveillance technology sector.[1] This ecosystem, shaped through decades of settler-colonial domination and military occupation, enables the rapid development, refinement, and deployment of digital tools designed to monitor, classify, and eliminate.[2] Technologies are first tested on Palestinians, particularly in Gaza and the West Bank, then refined for export.[3] As Loewenstein argues in his 2023 book on Palestine as a laboratory, the Israeli occupation has been transformed into a profitable model of surveillance capitalism. Palestinians have become the subjects of what is now widely identified as the world's first AI-powered genocide.[4]

Israeli security companies have long exceeded the role of arming repressive regimes, instead embedding themselves within neoliberal security projects that render militarized expertise as mobile capital, circulating through transnational markets in ways that reproduce and reinforce U.S.-centred hegemony.[5] Israeli companies often reach markets shunned by other suppliers.[6] Across Latin America, Africa, and Asia, Israel has consolidated a strategic niche through supplying states with integrated packages of military and digital surveillance infrastructures.[7] The occupied Palestinian territories have provided the showcase: techniques of population control honed in East Jerusalem[8], the West Bank[9], and Gaza[10] – constant biometric surveillance, predictive policing, high-tech walls and drones – are repackaged for export as "homeland security" products.[11]

1 Privacy International, "Big Tech's Bind with Military and Intelligence Agencies," Privacy International, October 1, 2025, https://privacyinternational.org/long-read/5683/big-techs-bind-military-and-intelligence-agencies.

2 Ihab Maharmeh, "AI as a Tool for Settler-Colonial Projects: How Israel Employs AI to Intensify Colonial Dominance under the Pretext of Counterterrorism," Critical Studies on Terrorism (2025): 1–24, https://doi.org/10.1080/17539153.2025.2603049

3 Antony Loewenstein, The Palestine Laboratory: How Israel Exports the Technology of Occupation around the World (London: Verso Books, 2023).

4 Amber Rahman, "Explainer: The Role of AI in Israel's Genocidal Campaign against Palestinians," Institute for Palestine Studies, 2019, https://www.palestine-studies.org/en/node/1656285.

5 Shir Hever, The Privatization of Israeli Security (London: Pluto Press, 2018).

6 Justice For Myanmar, "Israel's CAA Industries Ltd Suspected to Have Aided and Abetted the Myanmar Military's War Crimes and Crimes against Humanity," June 8, 2023, https://www.justiceformyanmar.org/stories/israels-caa-industries-ltd-suspected-to-have-aided-and-abetted-the-myanmar-militarys-war-crimes-and-crimes-against-humanity

7 Who Profits, "Repression & Diplomacy," Who Profits Research Center, 2022, https://www.whoprofits.org/publications/report/52?repression-diplomacy

8 Sophia Goodfriend, The Expansion of Digital Surveillance in Jerusalem and Impact on Palestinians Rights (7amleh – The Arab Center for Social Media Advancement, Summer and Fall 2021), https://7amleh.org/storage/Digital%20Surveillance%20Jerusalem_7.11.pd

9 Amnesty International, "Ban the Scan," https://banthescan.amnesty.org/opt/

10 Business & Human Rights Resource Centre, "Palantir Allegedly Enables Israel's AI Targeting amid Israel's War in Gaza, Raising Concerns over War Crimes," Business & Human Rights Resource Centre, https://www.business-humanrights.org/en/latest-news/palantir-allegedly-enables-israels-ai-targeting-amid-israels-war-in-gaza-raising-concerns-over-war-crimes/.

11 Rohan Talbot, "Automating Occupation: International Humanitarian and Human Rights Law Implications of the Deployment of Facial Recognition Technologies in the Occupied Palestinian Territory," International Review of the Red Cross 102, no. 914 (2020): 823–49, https://doi.org/10.1017/s1816383121000746.

Indeed, by the mid-2010s Israel was known as the global "homeland security capital"[12], hosting the most surveillance-tech companies per capita in the world.[13]

Critically, Israel's Ministry of Defense actively structures this ecosystem. Through its R&D Directorate (MAFAT), the MoD links military demand to startup-driven innovation, translating operational needs into technological development pipelines.[14] Operating as a joint interface between the Ministry and the IDF's technological apparatus, MAFAT coordinates across major defense firms, including Israel Aerospace Industries, Rafael, and Elbit Systems, while integrating universities and private-sector actors into a unified production network.[15]

By 2025, this public-private synergy reached new heights where over 130 Israeli startups were directly integrated into the military's operations after the war on Gaza began in 2023[16], many focusing on AI, autonomy, and sensing systems. Defense-tech startups working with MAFAT attracted over $1 billion in funding – more than in all previous years combined.[17] As global military spending reaches $2.7 trillion, Israeli defense technologies are increasingly absorbed into global markets as high-yield investments.[18] War, in turn, becomes a stable field for accumulation.[19]

More than thirty surveillance firms currently operate in Israel, many founded or staffed by veterans of Unit 8200, a signals intelligence unit centered on the interception and analysis of electronic communications and digital infrastructures.[20] These firms are deeply embedded in military data infrastructures and aligned with state priorities, forming what Sophia Goodfriend describes as an "intelligence-industrial complex."[21]

Within this configuration, AI systems such as Lavender, Gospel, and Where's Daddy draw on extensive surveillance datasets to generate automated targeting lists, compressing the interval between data extraction and lethal action and thereby accelerating both the speed and scale of airstrikes. As

12 Neve Gordon, "Israel's Emergence as a Homeland Security Capital," in Surveillance and Control in Israel/Palestine: Population, Territory and Power, ed. Elia Zureik, David Lyon, and Yasmeen Abu-Laban (London: Routledge, 2010), 18.

13 Visualizing Palestine, "Fact Sheet: The Israeli Cyber Industry," Medium, August 30, 2022, https://visualizingpalestine.medium.com/fact-sheet-the-israeli-cyber-industry-d2a64b43094

14 Dean Shmuel Elmas, "Defense Ministry Orders Boost Israeli Startups," Globes, January 21, 2026, https://en.globes.co.il/en/article-defense-ministry-orders-boost-israeli-startups-1001532687

15 Al-Shabaka: The Palestinian Policy Network, "Insulation Not Isolation: Israel's Super-Sparta War Economy," 2026, https://al-shabaka.org/briefs/insulation-not-isolation-israels-super-sparta-war-economy/

16 Dean Shmuel Elmas, "Israeli Defense Tech Startups Attract over $1b in Investment," Globes, December 8, 2025, https://en.globes.co.il/en/article-israeli-defense-tech-startups-attract-over-1b-in-investment-1001528671

17 Dean Shmuel Elmas, "Israeli Defense Tech Startups Attract over $1b in Investment," Globes, December 8, 2025, https://en.globes.co.il/en/article-israeli-defense-tech-startups-attract-over-1b-in-investment-1001528671

18 Lisya Bahar Manoah, "Rising Defense Spending: Fueling a Deep Tech Boom in 2026," Forbes, March 3, 2026, https://www.forbes.com/councils/forbesfinancecouncil/2026/03/03/rising-defense-spending-fueling-a-deep-tech-boom-in-2026/

19 Michael Kwet, "Digital Colonialism: The Evolution of US Empire," TNI Longreads, March 4, 2021, https://longreads.tni.org/fr/digital-colonialism-the-evolution-of-us-empire.html

20 7amleh – The Arab Center for the Advancement of Social Media, Israel's Surveillance Industry and Human Rights: Impact on Palestinians and Worldwide (December 2023), https://7amleh.org/storage/Israel%E2%80%99s%20Surveillance%20Industry%20english4.pdf.

21 Sophia Goodfriend, "Militarised AI," London Review of Books (blog), January 28, 2025, https://www.lrb.co.uk/blog/2025/january/militarised-ai.

Goodfriend says, this is enabled by the growing indistinction between technology companies and intelligence agencies. Reservists drawn from major firms, including Google, Microsoft, and Amazon, have been mobilized into military operations while facilitating access to the infrastructures they help build in the private sector.[22] Cloud platforms, AI models, and large-scale data storage systems are thus directly integrated into military workflows, processing vast volumes of information to inform targeting decisions.[23] The result is not only a convergence of corporate and military domains, but a more consequential collapse, which is the translation of mass data collection into an expanding, never-ending and continuously generated field of targets, intensifying the scale and tempo of violence.

The dynamics outlined above are reflected in the practices of surveillance firms themselves, whose operations often rely on opaque and legally ambiguous infrastructures, brought to light primarily through investigative reporting or legal challenge. These firms operate within an expanding transnational ecosystem, making mass data extraction both more pervasive and less bounded by territorial limits. Firms such as the 9500 Group, led by former Israeli intelligence officers and represented in Cybersec Asia 2026[24], a major regional cybersecurity forum that brings together governments, technology firms, and security actors across the Asia-Pacific, exemplify how surveillance firms extend their reach through transnational networks and align with broader geopolitical agendas.

Drawing on data from Start-Up Nation Central, alongside analysis of Ministry of Defense export frameworks, procurement channels, and corporate disclosures, this paper identifies a concentrated set of actors operating at the intersection of surveillance and security technologies. Rather than relying on a single dataset, it triangulates across multiple sources to map how these entities function within broader economic and security infrastructures. While often described as "startups," these actors are more accurately understood as firms in the economic sense. A corporation denotes a legal entity that owns assets and enters contracts, whereas a firm refers to the underlying organization of production i.e. the coordination of capital, labor, and technology through a network of contractual relations[25]. This distinction is central to the analysis. By examining legal form, funding structures, and self-representation, all through the lens of industrial policy, the paper traces the infrastructures through which surveillance technologies are operationalized across borders.

The paper advances three main arguments. First, it argues that surveillance firms such as Toka Group and Corsight AI must be understood as integral components of Israel's industrial policy. Conventionally, industrial policy refers to the strategic shaping of economic sectors through state support, including investment, procurement, regulation, and export facilitation. In the Israeli case, however, this policy is explicitly organized around security and

22 Ibid.

23 Mahmoud Javadi, "Infrastructural Entanglement and Cloud Hyperscalers in Contemporary Warfare: Insights from Ukraine, Israel and Taiwan," Contemporary Security Policy 47, no. 2 (2026): 469–506, https://doi.org/10.1080/13523260.2025.2593247

24 Cybersec Asia, "Speakers," Cybersec Asia, accessed February 1, 2026, https://cybersec-asia.net/cybersec-asia-speakers/.

25 Jesús Alfaro Águila-Real, "Corporations Are Not Firms," Oxford Business Law Blog, May 29, 2017, https://blogs.law.ox.ac.uk/business-law-blog/blog/2017/05/corporations-are-not-firms

militarization.[26] Firms such as Toka and Corsight AI do not position themselves as standalone service providers, but as branched-out actors within ecosystems linking state agencies, private capital, and international institutions. This positioning enables them to function as intermediaries that translate state priorities into marketable technologies while extending those technologies across borders. Understanding these actors as firms thus shifts the analytical focus away from the state as a singular unit, toward the infrastructures through which surveillance is produced and deployed across domains such as warfare, policing, and border control.[27]

Second, the paper argues that this firm-based configuration facilitates the expansion of surveillance beyond territorial boundaries, generating forms of control that are not confined to physical borders. While existing scholarship has emphasized how public–private partnerships blur distinctions between civilian and military infrastructures[28], this paper suggests that Israeli industrial policy simultaneously depends on maintaining a degree of discursive separation, i.e. on the narrative and self-description level. This separation enables firms to access new markets, especially where direct political or economic ties with Israel are constrained. Through the global circulation of firms, surveillance infrastructures are extended into new geographies, enabling forms of data extraction that are effectively unbounded. In this sense, the expansion of surveillance technologies also entails an expansion of Israeli security logics, what might be understood as an extended "security zone", a key narrative and tool used by Israel in recent years, beyond territorially bounded contexts.[29] Through access to transnational data infrastructures, these firms contribute to widening the scope within which populations, including Palestinians and those in solidarity with them, can be monitored, targeted, and governed, under the prevailing discourse of "security."[30]

Third, the paper argues that multilateral development and governance institutions function as key interfaces in this process. For example, Toka, integrated into World Bank-supported digital governance initiatives, and Corsight AI, which partners with police agencies across Europe and Asia, illustrate how technologies developed within contexts of military occupation are reframed as tools of "capacity-building" and "digital governance."[31] While this dynamic has been documented in existing scholarship[32], this paper extends the analysis by foregrounding the emergence of new markets

26 Seher Bulut, "Israel's Defense Industry Policy: Security-Centered Transformation, Unregulated Armament and Ethics of Accountability," CENK 1, no. 2 (2025), https://doi.org/10.5281/zenodo.18082695.

27 Milan Babić, Jan Fichtner, and Eelke M. Heemskerk, "States versus Corporations: Rethinking the Power of Business in International Politics," The International Spectator: Italian Journal of International Affairs 52, no. 4 (2017): 20–43, https://doi.org/10.1080/03932729.2017.1389151.

28 Joseph F. Getzoff, "Start-up Nationalism: The Rationalities of Neoliberal Zionism," Politics & Political Theory 38, no. 5 (2020), published March 19, 2020.

29 Binoy Kampmark, "De Facto Occupation: Israel's Security Zone Strategy," Countercurrents, April 19, 2025, https://countercurrents.org/2025/04/de-facto-occupation-israels-security-zone-strategy/

30 Elia Zureik, "Strategies of Surveillance: The Israeli Gaze," Jerusalem Quarterly, no. 66 (June 2016): 12, https://doi.org/10.70190/jq.i66.p12

31 Eugenio V. Garcia, "Technology for Whom and for What? A Global South View of Tech Diplomacy," Global Policy, published July 7, 2025, https://doi.org/10.1111/1758-5899.70024.

32 Tactical Tech, "Systematized Supremacy: Witnessing How Tech Is Used to Conquer and Destroy," Tactical Tech, September 22, 2025, https://tacticaltech.org/news/insights/systematized-supremacy/

structured around the global circulation of Israeli security logics, and the expansion of their operational reach.

Focusing on Toka Group and Corsight AI, the paper does not seek to compare products or market share, but to examine how these firms operate within this broader configuration. They exemplify the entanglement of technical, military, and political domains that characterizes the contemporary surveillance regime, while maintaining a strategic discursive distance from Israeli state actors but not from the broader objectives those actors pursue.

The paper proceeds in five parts. It begins by outlining the theoretical and methodological framework. It then situates Toka and Corsight AI within Israel's cyber public–private ecosystem. The third section analyzes how these firms present themselves to governments, investors, and global publics, and how these narratives both reflect and shape Israeli industrial policy.

CONCEPTUAL FRAMEWORK

This section develops the conceptual framework through which the paper's three central arguments are understood. To develop this framework, the section brings together literatures surveillance studies, and digital/data imperialism and colonialism, while also grounding the analysis in scholarship on industrial policy, and the organizational form of the firm.

Surveillance in this paper is defined as both a governance practice and a commodified capability[33] i.e. a socio-technical assemblage[34] drawing together state agencies, legal regimes, infrastructures, datasets, labour pipelines, and corporate marketing.[35] This framing is consistent with (and helps the paper explicitly mobilise) empirical work documenting how surveillance in Palestine operates across layered infrastructures of population control[36], and how algorithmic/biometric systems are bound up with the political imperatives of settler expansion.[37]

In this context, particularly with the rapid expansion of AI-driven surveillance technologies and imperialist expansionist projects[38], industrial policy has re-emerged as a central pillar of contemporary economic governance. It is no longer limited to developmental or protectionist aims, but is increasingly oriented toward security imperatives and militarised forms of state

33 Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (New York: PublicAffairs, 2019).

34 Gavin Sullivan, "Law, Technology, and Data-Driven Security: Infra-Legalities as Method Assemblage," Journal of Law and Society (March 2022), https://doi.org/10.1111/jols.12352.

35 Daniel Marciniak, "Infrastructure Shortcuts: The Private Cloud Infrastructure of Data-Driven Policing and Its Political Consequences," in States of Surveillance: Ethnographies of New Technologies in Policing and Justice, ed. Maya Avis, Daniel Marciniak, and Maria Sapignoli (London: Routledge, 2025).

36 Nadera Shalhoub-Kevorkian, Security Theology, Surveillance and the Politics of Fear (Cambridge: Cambridge University Press, 2015)

37 Sarah Fathallah, "Algorithmic Death-World: Artificial Intelligence and the Case of Palestine," Public Humanities 2 (2026): e7, https://doi.org/10.1017/pub.2025.10113.

38 Neema Iyer, Garnett Achieng, Favour Borokini, and Uri Ludger, Automated Imperialism, Expansionist Dreams: Exploring Digital Extractivism in Africa (Kampala: Pollicy, June 2021), https://pollicy.org/wp-content/uploads/2021/10/Automated-Imperialism-Expansionist-Dreams-Exploring-Digital-Extractivism-in-Africa_2-1.pdf

strategy.[39] Recent scholarship shows that governments are deploying coordinated interventions,ranging from subsidies and public procurement to export controls and R&D financing, within globally integrated production systems, where firm-level activity is deeply embedded in cross-border value chains.[40] In this context, industrial policy, even with tech and specifically AI, operates as a mechanism for structuring entire ecosystems of production, investment, and war-oriented high-tech, as economic policy and national security have become increasingly indistinguishable.[41]

This paper builds on this literature by advancing the concept of militarized industrial policy, as a form of industrial policy in which the development, organization, and global circulation of economic sectors are explicitly structured around military imperatives, security logics, and geopolitical strategy.[42] For Israel, this is not a recent development but a historically embedded formation. As Tariq Dana argues, Israel's war economy is not episodic but systemic, rooted in pre-state militarized institution-building and sustained through a tight integration of military, technological, and economic infrastructures.[43] Militarized industrial policy, in this sense, describes a condition in which military priorities do not merely influence economic development but actively organize it.

Using the lens of industrial policy requires an understanding of how this militarized mechanism is taking shape legally, financially, and discursively.[44] This is why in this paper there is a precise conceptual distinction between firm, company, and related legal categories.[45] Under Israeli law, a "company" is a specific statutory form incorporated under the Companies Law, while "corporation" functions more broadly as an umbrella term corresponding to the legal notion of a "body corporate," a juristic person capable of holding rights and obligations.[46] By contrast, "startup" is not a legal category but a lifecycle descriptor used in investment and policy frameworks. Crucially, the "firm" is not itself a legal entity but an economic organization that has a configuration of contracts, production factors, and governance relations that coordinates capital, labor, and technology.

39 Jostein Hauge, "Industrial Policy Returns as a Weapon of National Security," The Global Currents, December 16, 2025, https://www.theglobalcurrents.com/p/industrial-policy-returns-as-a-weapon.

40 Jostein Hauge, Bruno Houtzager, and Alessandro Julian Hörmann, "The New Economic Nationalism: Industrial Policy and National Security in the United States, China, and the European Union," Geoforum 166 (November 2025): 104382, https://doi.org/10.1016/j.geoforum.2025.104382

41 AI Now Institute, AI Nationalism(s): Global Industrial Policy Approaches to AI, March 12, 2024, https://ainowinstitute.org/publications/research/ai-nationalisms-global-industrial-policy-approaches-to-ai

42 Ulises A. Mejias and Nick Couldry, Data Grab: The New Colonialism of Big Tech and How to Fight Back (Chicago: University of Chicago Press, 2024).

43 Tariq Dana, "Merchants of Death: Israel's Permanent War Economy," Security in Context, January 29, 2024, https://www.securityincontext.org/posts/merchants-of-death-israels-permanent-war-economy.

44 Susannah Glickman, "AI and Tech Industrial Policy: From Post-Cold War Post-Industrialism to Post-Neoliberal Re-Industrialization," AI Now Institute, March 12, 2024, https://ainowinstitute.org/publications/ai-and-tech-industrial-policy-from-post-cold-war-post-industrialism-to-post-neoliberal-re-industrialization

45 Jesús Alfaro Águila-Real, "Corporations Are Not Firms," Oxford Business Law Blog, May 29, 2017, https://blogs.law.ox.ac.uk/business-law-blog/blog/2017/05/corporations-are-not-firms.

46 Israel Business Connection, "Company Registration," Israel Business, accessed March 1, 2026, http://www.israelbusiness.org.il/startingyourbusiness/companyregistration.

This distinction is analytically decisive. According to the companies registrar, entities such as Corsight AI Ltd (founded 2019) and Cortica Ltd (founded 2007) are formally registered as private companies, yet they operate as subsidiaries within larger firms embedded in complex networks of investment, security governance, and transnational contracting, including military agreements. Their structure, often involving group formations, subsidiaries, and board-level ties to investors and former military or intelligence figures, cannot be captured by legal form alone.[47] Instead, the firm concept makes visible how these actors function as operational nodes within a broader militarized economy.

This becomes clearer when looking at the regulatory environment in which these firms operate. In Israel, defence exports are regulated by the Defense Export Control Agency (DECA) under the 2007 Defence Export Control Law, which requires licenses for marketing and exporting defence-related technologies and aligns with international regimes such as Wassenaar and the Missile Technology Control Regime. Alongside this, dual-use exports are overseen by the Ministry of Economy, while cyber exports are subject to increasingly strict end-user requirements.[48]

Recent global trade control developments, including updates in late 2025, show that these export controls are no longer limited to national regulation but are part of a broader system of international economic governance. Firms are now required to meet stricter compliance standards across borders, including more rigorous end-user checks, due diligence processes, and coordination with allied regulatory frameworks. This extends responsibility across the entire supply chain, meaning firms must account not only for who they sell to directly, but also how technologies are used, transferred, and circulated beyond the initial transaction.[49]

Within this increasingly dense regulatory landscape, the firm form becomes particularly significant. These actors are not confined to a single institutional or territorial structure; rather, they operate through layered contractual arrangements such as subsidiaries, partnerships, licensing agreements, joint ventures, and service provision models that can be reconfigured depending on regulatory environments. This makes it possible to route technologies, expertise, and data through multiple legal and geographic channels, even under conditions of export control. Instead of functioning as vertically integrated entities, firms distribute their operations, sensitive components may be developed in one entity, held in another, and deployed through partnerships with third parties. What emerges here is the material infrastructure of a militarized industrial policy, a system in which the state's security priorities are diffused through firms that operationalise, extend, and globalise them. In this configuration, the firm form becomes the mechanism through which war and surveillance are made scalable and transnational, transforming

47 William Hamilton Byrne, Thomas Gammeltoft-Hansen, and Nora Stappert, "Legal Infrastructures: Towards a Conceptual Framework," German Law Journal 25, no. 8 (2024): 1229–46, https://doi.org/10.1017/glj.2024.78

48 State Comptroller and Ombudsman of Israel, State Comptroller Report 76B (December 2025), https://library.mevaker.gov.il/sites/DigitalLibrary/Documents/2025/2025-12/EN/2025.12-76B-203-EN.pdf

49 Shibolet & Co., "Developments in Global Trade Controls: October–December 2025," Shibolet & Co., January 20, 2026, https://www.shibolet.com/en/developments-in-global-trade-controls-october-december-2025/.

what might appear as fragmented commercial activity into a coherent infrastructure of control.[50]

Companies in cyber and defence-adjacent sectors tend to incorporate as Israeli private limited companies to align with licensing requirements, often segment controlled technologies into subsidiaries, i.e. firms, to manage regulatory exposure, and design governance structures to mitigate risks related to disclosure of sensitive technologies.[51] Militarized industrial policy then operates through the firm form itself, firms become the institutional vehicles through which military technologies are developed, tested, licensed, and exported, so, firms, in both discursive and legal definitions, function simultaneously as economic actors, security intermediaries, and instruments of geopolitical strategy.

METHODOLOGY

Studying cyberoffensive firms requires working through structured opacity. These actors operate across export-control regimes, classified partnerships, nondisclosure agreements, and deliberately sanitized corporate language that obscures both capabilities and use cases. Direct access to information is limited as key contracts are undisclosed, technical specifications are partial, and governance arrangements are often fragmented across jurisdictions. As a result, the analysis cannot rely on any single source, but must instead reconstruct these systems through dispersed and incomplete traces.

To address these constraints, this research adopts a multi-source methodological approach that treats opacity itself as an analytical condition. It triangulates across corporate materials, media reporting, regulatory frameworks, and movement-generated knowledge to map how these firms operate and how they represent themselves. This includes examining founders' biographies, venture capital networks, corporate filings (where available), export licenses, and public-private partnerships; analyzing media coverage across Arabic, English, and Hebrew sources; and reviewing Israeli export governance through materials from SIBAT and related state bodies. It also draws on company-facing outputs such as pitch decks, promotional videos, and security expo presentations to understand how these firms construct their public narratives, alongside critical analyses produced by researchers and digital rights organizations.

Methodologically, the research combines thematic and discourse analysis to examine how firms such as Toka and Corsight narrate their technologies across these materials. Thematic analysis identifies recurring terms while discourse analysis situates these within broader frameworks that obscure the origins and functions of the technologies. This approach shifts the focus away from product descriptions toward the political and economic logics that structure how these systems operate in different governance contexts.

50 Laleh Khalili, "How Empire Operates: An Interview with Laleh Khalili," Viewpoint Magazine, February 1, 2018, https://viewpointmag.com/2018/02/01/empire-operates-interview-laleh-khalili/.

51 Haim Ravia and Dotan Hammer, "Israel Publishes Draft Bill on National Cyber Protection," Pearl Cohen, January 28, 2026, https://www.pearlcohen.com/israel-publishes-draft-bill-on-national-cyber-protection/

However, rather than attempting to overcome opacity, this methodology works through it. The partial, mediated nature of the available data is not treated as a limitation alone, but as indicative of how these firms operate.

Why Toka and Corsight?

This research focuses on Toka Group and Corsight AI because they are analytically revealing cases. Toka Group is a cyber intelligence firm that provides governments with capabilities for accessing and extracting data from connected devices, positioning "access" itself as a tool of governance. Corsight AI, a subsidiary of Cortica, develops advanced facial recognition systems designed for identification, tracking, and real-time monitoring across security and policing contexts. These two firms provide concrete entry points through which the wider processes of the surveillance economy can be traced. Their selection is therefore methodological as they allow the paper to examine how militarized industrial policy operates in practice, while remaining attentive to the fact that they represent only part of a larger ecosystem that includes state institutions, financial actors, military infrastructures, and global markets.

Both firms are private-sector actors that operate within, and simultaneously beyond, the state. Formally registered as private companies, they function as firms embedded in transnational networks of investment, regulation, and security governance. They hold export licenses, participate in international security forums, and position themselves as partners in domains such as digital governance, law enforcement, forensics, and border control. This positioning is central to their role within militarized industrial policy where they operate as intermediaries that translate state security priorities into scalable and marketable technologies. Their organisational form as firms allows them to move across jurisdictions, as they are based in multiple countries including the US. This allows them to embed themselves in diverse institutional settings, and access markets that might otherwise be politically restricted.

The growth of firms like Toka and Corsight is thus enabled by an alignment between state priorities, venture capital, and regulatory frameworks, including export controls and procurement systems that facilitate their integration into international markets.

At the same time, these firms illuminate how surveillance operates as both governance and infrastructure. Their technologies emerge within a context of managing and controlling Palestinian populations, yet are designed from the outset to be scalable and transferable. What is developed as a mechanism of control is reconfigured into a generalised model of governance. In this sense, firms like Toka and Corsight extend the logics of surveillance into new contexts, including and not limited to the UK and Kenya, among other countries.. Focusing on these firms therefore allows the paper to trace how militarized industrial policy is enacted through the firm form, showing how surveillance is then circulated as global commodity.

TOKA

Toka is a private Israeli firm that explicitly "links the worlds of cyberoffense, active intelligence and smart surveillance." Since its founding in 2018, it has been positioned as a state-adjacent security exporter. Toka is formally listed with SIBAT[52], the International Defense Cooperation Directorate of Israel's Ministry of Defense, as an official defense exporter in the categories of "cyber defense" and "cyber intelligence" (confirmed in 2025). In other words, the Israeli state itself recognizes Toka's products as part of its defense export portfolio.

From the outset, Toka has pitched itself "as a one-stop hacking shop for governments"[53], as a firm that designs national "cyber resilience" and then supplies the tools to penetrate, monitor, and manipulate the very infrastructures it helps to build. It sits at the intersection of three economies: the Israeli military–intelligence complex, US venture capital, and multilateral development finance (including the World Bank, Inter-American Development Bank, and UN agencies), which together convert offensive cyber capabilities into exportable "capacity-building" projects in the global South and among US allied states.[54]

1. ORIGINS, OWNERSHIP, AND POSITION

Toka's founding team crystallizes the pipeline between Israeli military/intelligence institutions and the private cyber industry.[55] The company was co-founded in 2018 by former Prime Minister and former IDF Chief of General Staff Ehud Barak and Brig. Gen. (res.) Yaron Rosen, former head of the IDF's Cyber Staff.[56] Barak's long tenure atop Israel's security apparatus (including oversight of Mossad and military intelligence as Defense Minister) anchors Toka firmly in the orbit of state covert operations. Rosen brings direct experience in designing and deploying offensive and defensive cyber capabilities for the IDF.[57]

They are joined by co-founders Alon Kantor and Kfir Waldman, who represent the "civilian" side of Israel's security-tech ecosystem, with careers built in companies like Check Point and Cisco, firms themselves rooted in Unit 8200 networks.58 Waldman now serves as CEO. Toka's chief architect of its hacking suite, Moty Zaltsman, came from the Netanyahu's Office

52 SIBAT is the International Defense Cooperation Directorate of the Israel Ministry of Defense, that has the goal of promoting and marketing Israeli arms exports around the world.

53 Thomas Brewster, "Alexa, Are You a Spy? Israeli Startup Raises $12.5 Million So Governments Can Hack IoT," Forbes, July 15, 2018, https://www.forbes.com/sites/thomasbrewster/2018/07/15/toka-will-hack-internet-of-things-for-government-intelligence-agencies/

54 Charles Rollet, "a16z-Backed Toka Wants to Help US Agencies Hack into Security Cameras and Other IoT Devices," Yahoo Finance (originally published in TechCrunch), December 6, 2024, https://au.finance.yahoo.com/news/a16z-backed-toka-wants-help-183623502.html

55 Toka, "Company Leadership," Toka Group (archived December 19, 2021), https://web.archive.org/web/20211219162602/https://www.tokagroup.com/company#leadership (for former governance structure).

56 Yasmin Yablonko, "Ehud Barak-Founded Cybersecurity Co Toka Raises $12.5m," Globes, July 16, 2018, https://en.globes.co.il/en/article-ehud-barak-founded-cybersecurity-co-toka-raises-125m-1001246322

57 Yonah Jeremy Bob, "Ex-IDF Cyber Intel Official: How to Carry Out a Cyber Offense Attack," The Jerusalem Post, September 14, 2021, https://www.jpost.com/israel-news/ex-idf-cyber-intel-official-how-to-carry-out-a-cyber-offense-attack-677173

58 Corporate Watch, "Check Point Software: Ex-Israeli Military Spooks Profiting from the Cyber Security Industry," Corporate Watch, November 25, 2019, https://corporatewatch.org/check-point-software-ex-israeli-military-spooks-profiting-from-the-cyber-security-industry/.

tech unit and worked on offensive intelligence technologies; he was closely associated with Netanyahu-era offensive tech projects before his biography was quietly sanitized after critical coverage.[59] Another senior figure, Nir Peleg, serves as VP for strategic projects and previously headed R&D at the National Cyber Directorate's elite tech unit[60], working closely with Tal Goldstein (a key architect of Israel's cyber strategy in global forums such as the World Economic Forum).[61]



Toka's corporate leadership and board further entrench these ties. While Barak stepped back from an active role around 2020-2024, he remained a central early figure and symbol of the company's strategic positioning. The board includes Rosen himself and tech investor Lior Susan, a former IDF special forces officer turned venture capitalist.[62] Recent reporting by Forbes further highlights Barak's continued interest in mobilising capital for Toka alongside his broader portfolio of ventures. Ahead of the company's public launch in 2018, Barak actively sought investment and strategic backing for

59 Corporate Watch, "Check Point Software: Ex-Israeli Military Spooks Profiting from the Cyber Security Industry," Corporate Watch, November 25, 2019, https://corporatewatch.org/check-point-software-ex-israeli-military-spooks-profiting-from-the-cyber-security-industry/.

60 Toka's 'About US' page.

61 Jennifer L. Schenker, "Interview of the Week: Tal Goldstein, World Economic Forum Centre for Cybersecurity," The Innovator, https://theinnovator.news/interview-of-the-week-tal-goldstein-world-economic-forum-centre-for-cybersecurity/.

62 Samantha Huang, "He Went From Working on a Banana Farm to Selling His First Company to Cisco in the Span of a Decade: Meet Lior Susan, Founding Partner of Eclipse Ventures," EVCA, March 1, 2021, https://evca.org/content/he-went-from-working-on-a-banana-farm-to-selling-his-first-company-to-cisco-in-the-span-of-a-decade-meet-lior-susan-founding-partner-of-eclipse-ventures.

Toka, including outreach to high-net-worth individuals with government connections, explicitly framing the company as "built for governments as clients." While these efforts did not necessarily translate into direct investment, they underscore how Toka was positioned from the outset as a state-facing enterprise requiring both capital and political access to scale.[63]

The investor base maps directly onto US-Israeli tech and security alliances. Andreessen Horowitz (a16z) is a lead backer[64]; co-founder Marc Andreessen sits on the Meta board and was named as a defendant in privacy litigation around Meta's non-compliance with US regulatory orders, highlighting how Toka is entangled with firms already accused of large-scale data abuses.[65] Entrée Capital, mentioned in Toka's 'investors' section, is led by Aviad Eyal and Ran Achituv, brings additional signals-intelligence lineage as Achituv previously worked in satellite-based SIGINT and held senior roles at Amdocs and Comverse, both linked to earlier espionage controversies targeting US communications.[66]

Former Haaretz reporting indicates that Toka's contracts were not purely market-driven but were planned and supported by an inter-ministerial committee set up under Netanyahu to "realize the potential of international development" for Israeli cyber firms. In practice, this means Toka is used as an instrument of Israeli industrial and foreign policy. Its listing under SIBAT, its staffing with IDF and intelligence veterans, and its coordination with the Ministry of Defense all position Toka as a privatized extension of Israel's offensive cyber apparatus rather than a neutral "cyber consultancy."[67]

In late 2025, under CEO Gregg Smith, the company moved its headquarters to the U.S. while maintaining a subsidiary in Israel. This reflects the flexibility of the firm form, Toka can reorganise across jurisdictions to align with key security, regulatory, and political environments.[68]

2. FROM "LAWFUL INTELLIGENCE" TO IOT WEAPONRY

Toka's public narrative is carefully constructed. The company claims to "provide law enforcement, homeland security, defense, and intelligence agencies with software and a platform to aid, accelerate, and simplify their investigations and operations,"[69] so they can "lawfully, quickly, and easily access the information they require to keep people, places, and communities safe." Its marketing materials emphasize "ethical hacking," "lawful

63 Thomas Brewster, "Epstein Could Have Made $100 Million On A Secret Police Tech Investment," Forbes, February 10, 2026, https://www.forbes.com/sites/thomasbrewster/2026/02/10/epstein-police-surveillance-investments-with-ehud-barak/

64 Andreessen Horowitz, "Investment List," a16z, accessed April 1, 2026, https://a16z.com/investment-list/

65 Henry Chandonnet, "Marc Andreessen Says Being Controversial Gives His VC Firm an 'Incredible Competitive Advantage,'" Business Insider, January 12, 2026, https://www.businessinsider.com/marc-andreessen-controversial-competitive-advantage-venture-capital-2026-1

66 James Bamford, "Shady Companies With Ties to Israel Wiretap the U.S. for the NSA," Wired, April 3, 2012., https://www.wired.com/2012/04/shady-companies-nsa/

67 Omer Benjakob, "This 'Dystopian' Cyber Firm Could Have Saved Mossad Assassins From Exposure," Haaretz, December 26, 2022, https://www.haaretz.com/israel-news/security-aviation/2022-12-26/ty-article-magazine/.premium/this-dystopian-cyber-firm-could-have-saved-mossad-assassins-from-exposure/00000185-0bc6-d26d-a1b7-dbd739100000.

68 Toka, "Toka Deepens Engagement with U.S. and Allied Government Partners, Names Gregg Smith CEO," February 26, 2026, https://tokagroup.com/news/toka-deepens-engagement-with-u-s-and-allied-government-partners-names-gregg-smith-ceo/

69 Toka's 'About US page'

interception," "forensics," "critical infrastructure protection," and "full-spectrum cyber strategies."[70] It presents itself as a partner helping governments build integrated cyber defense, secure smart cities, and enhance national resilience.

A company pitch deck obtained by Haaretz ournalists describes Toka as offering "previously out-of-reach capabilities" that "transform untapped IoT sensors into intelligence sources" for "intelligence and operational needs."[71]

In its own language on its website, Toka enables clients to:

- Discover and access security and smart cameras in a "targeted area."
- Stream and control cameras within that area over time.
- Target vehicles via connected car media systems, providing "car forensics and intelligence", including the geolocation and movement of vehicles.
- Gather visual intelligence from both "live or recorded videos."
- Alter audio and visual feeds to "mask on-site activities" during "covert operations."

Toka's systems are marketed as the tool a police force could use to remotely track a "terror attack" across a city by taking over urban camera networks. The same infrastructure, by design, enables covert collection and manipulation of visual data "without leaving a mark."

The most disturbing function highlighted in Toka's marketing is the ability to edit/alter, spoof, or delete video (and audio) recordings without leaving a forensic trace. This allows operators not only to monitor a scene but to retroactively erase their presence, fabricate evidence, or obscure state violence. This effectively destabilizes the concept of visual evidence, so if any CCTV footage can be silently altered, neither courts nor publics can trust what they see.

Technically, Toka's offensive model leverages common wireless attack surfaces. Many CCTV and IoT devices rely on shared chipsets (Bluetooth, Wi-Fi) sourced from third-party manufacturers; a vulnerability found in one chipset can be replicated across multiple brands.[72] Toka's interest in targeting devices over wireless interfaces means it can conduct tactical, localized attacks where an operator is physically proximate to the target network or remote attacks via the internet if the infrastructure is exposed.[73]

Unlike Pegasus, which focuses on phones, Toka moves toward environment-wide compromise. Reports by TechCrunch, among others, emphasize that Toka does not disclose vulnerabilities it discovers to vendors, instead

70 Ibid.

71 Omer Benjakob, "This 'Dystopian' Cyber Firm Could Have Saved Mossad Assassins From Exposure," Haaretz, December 26, 2022, https://www.haaretz.com/israel-news/security-aviation/2022-12-26/ty-article-magazine/.premium/this-dystopian-cyber-firm-could-have-saved-mossad-assassins-from-exposure/00000185-0bc6-d26d-a1b7-dbd739100000.

72 Keumars Afifi-Sabet, "Critical Supply Chain Flaw Exposes IoT Cameras to Cyber Attack," IT Pro, June 16, 2021, https://www.itpro.com/security/vulnerability/359899/critical-supply-chain-flaw-exposes-iot-cameras-to-cyber-attack.

73 Globes Correspondent, "Israeli Cybersecurity Co Toka Raises $25m," Globes, October 28, 2020, https://en.globes.co.il/en/article-israeli-cybersecurity-co-toka-raises-25m-1001347405.

hoarding zero-day exploits as strategic assets. This business model intentionally keeps global users insecure in order to preserve state clients' ability to break into their devices.[74]

Toka's own statements insist it serves only "trusted" governments, those with good "rule of law" and civil liberties records, through a "rigorous, annual review and approval process" guided by corruption and civil-liberties indices and supported by outside advisors (including prominent legal and economic figures such as Peter Schuck[75] and Jacob Frenkel[76]). This is the familiar "self-regulation" script that NSO Group deployed around Pegasus, a promise that powerful spyware will be used only for "legitimate" security purposes.[77] As mentioned in their website and previous press releases, there is nothing in Toka's code, governance structure, or licensing framework that meaningfully restricts how its tools are used in practice. In the absence of enforceable safeguards, its technologies can just as readily be deployed against anyone.

Taken together, Toka's claims and capabilities reveal a pattern. The public narrative is about lawful intelligence, crime-fighting, and critical infrastructure protection. The technical reality is a set of tools that allow states to silently control, manipulate, and erase the visual and digital traces of everyday life. The firm is best understood as a manufacturer of deniable power, it gives states the ability to see more and intervene without being 'seen'.[78]

Toka's self-representation in official defence export arenas reinforces this positioning. In its 2025 reporting, the company advertises itself as providing "first-of-their-kind software platforms for digital forensics and intelligence," explicitly targeting "trusted government, law enforcement, and security agencies." Its materials emphasize "lawful digital forensics tools and intelligence-gathering," alongside capabilities for "targeted intelligence" and "covert operations," presenting its technologies as enabling faster, scalable, and operationally efficient investigations.[79]

3. GLOBAL FOOTPRINT

Publicly and in responses to investigation, Toka insists it works only with the US and its allies, across sectors such as military, homeland security, intelligence agencies, law enforcement, border protection, and smart-city authorities.[80] It

74 Charles Rollet, "a16z-backed Toka Wants to Help U.S. Agencies Hack into Security Cameras and Other IoT Devices," TechCrunch, December 6, 2024, https://techcrunch.com/2024/12/06/a16z-backed-toka-wants-to-help-us-agencies-hack-into-security-cameras-and-other-iot-devices/.

75 "Peter H. Schuck," The Org, accessed April 1, 2026, https://theorg.com/org/toka/org-chart/peter-h-schuck.

76 "Yaakov Frenkel," The Org, accessed April 1, 2026, https://theorg.com/org/toka/org-chart/yaakov-frenkel.

77 John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, "Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware," Citizen Lab, June 19, 2017, https://citizenlab.ca/research/reckless-exploit-mexico-nso/.

78 Cormac, Rory, and Richard J. Aldrich. 2018. "Grey Is the New Black: Covert Action and Implausible Deniability." International Affairs 94 (3): 477–494. https://doi.org/10.1093/ia/iiy067.

79 Cybertoka Ltd. "First-of-their-kind software platforms for digital forensics and intelligence." Company profile in SIBAT (Israel Ministry of Defense) export materials.

80 Thomas Brewster, "Alexa, Are You a Spy? Israeli Startup Raises $12.5 Million So Governments Can Hack IoT," Forbes, July 15, 2018, https://www.forbes.com/sites/thomasbrewster/2018/07/15/toka-will-hack-internet-of-things-for-government-intelligence-agencies/

also markets advisory services to national Computer Emergency Response Teams (CERTs) and to private-sector critical infrastructure operators.[81]

CLIENT GEOGRAPHIES AND SECTORS

Israel

Toka's first and foundational client is the Israeli state. By 2021 it reportedly held contracts worth several million dollars with Israeli security agencies. Its products are coordinated with the Ministry of Defense, and its export approvals are treated as part of Israel's wider arms-control regime.[82]

Nigeria

In 2020, Toka was selected by the World Bank to advise Nigeria's government on designing and bolstering national cyber resilience. Under this World Bank-funded project, Toka participated in building Nigeria's cybersecurity frameworks, technical capabilities, and skills, including work with the national CERT and private companies.[83]

Moldova

Also in 2020, Toka obtained a World Bank-financed contract in Moldova to identify cybersecurity gaps in the public sector and propose a strategy to improve readiness. Though Moldova is small, the engagement demonstrated how Israeli cyber firms can leverage multilateral funding to enter Eastern European state infrastructures.[84]

Chile

In 2020, the Chilean government and the Inter-American Development Bank chose Toka to advise on national cybersecurity readiness and operational capacity building. Chile hosts one of the largest Palestinian diasporas globally and has strong domestic support for Palestine; Toka's insertion in Chile's security apparatus therefore carries clear geopolitical resonance for Israel.[85]

Ghana

Toka has also secured a World Bank contract with Ghana under the same global cybersecurity capacity-building program, extending its footprint in West Africa.[86]

81 Whitney Webb, "Meet Toka, the Most Dangerous Israeli Spyware Firm You've Never Heard Of," MintPress News, July 21, 2021, https://www.mintpressnews.com/meet-toka-the-most-dangerous-israeli-spyware-firm-youve-never-heard-of/278020/.

82 Becky Peterson, "The Founders of a Billion-Dollar Israeli Spyware Startup Accused of Helping Saudi Arabia Attack Dissidents Are Funding a Web of New Companies That Hack into Smart Speakers, Routers, and Other Devices," Business Insider, September 5, 2019, https://www.businessinsider.com/inside-the-israel-offensive-cybersecurity-world-funded-by-nso-group-2019-8.

83 IsraelDefense, "Israel's Toka Advising Nigeria on Cyber Security," February 24, 2020, https://www.israeldefense.co.il/en/node/42066.

84 Toka, "Toka Awarded World Bank-Financed Contract to Strengthen Moldova's National Cybersecurity Readiness," Yahoo Finance, September 10, 2020, https://finance.yahoo.com/news/toka-awarded-world-bank-financed-100000596.html.

85 Toka, "Toka Selected by Chile and Inter-American Development Bank to Assess and Support Chile's National Cybersecurity Readiness," GlobeNewswire, May 19, 2020, https://www.globenewswire.com/news-release/2020/05/19/2035462/0/en/Toka-Selected-by-Chile-and-Inter-American-Development-Bank-to-Assess-and-Support-Chile-s-National-Cybersecurity-Readiness.html

86 "Toka Scores $25 Million Series B to Enhance Cybersecurity of Gov't Organizations," Israel Defense, October 31, 2020, https://www.israeldefense.co.il/en/node/46195.

Mexico

Mexican government data indicates Toka is already operating in Mexico. Israeli media note growing Israeli business interest in Mexico under the current administration, signalling how cyber contracts are bundled with broader investment flows.[87]

Toka also references work or market development in the United States, Germany, Australia, Singapore, and Belgium.

ACCESS STRATEGIES

Beyond formal contracts, Toka's leadership has been actively expanding its markets. Yaron Rosen has been reported engaging with Moroccan officials in efforts to enter that market.[88] Company representatives have been visible at security and technology events such as Milipol, ISS World, Gitex in the UAE, and regional cyber conferences framed as Israel-UAE-Eastern Europe cybersecurity fora.[89] Toka's sales leadership has publicly signalled activity in the UAE and Asia, aligning with a broader Israeli push into Gulf and Asian cyber markets after normalization agreements.

Toka's global footprint is part of a larger political project. Israel has explicitly identified offensive cyber as a pillar of its industrial and foreign policy.[90] Domestically, Toka's tools support the expansion of surveillance and the erosion of accountability. They enable authorities to turn ubiquitous urban sensors into centralized intelligence systems, to track and intimidate dissent, and to erase or fabricate visual records of state violence. Internationally, the same tools can be used to monitor transnational movements, including solidarity networks, refugees, and activists. This is particularly salient given reporting that Israel and allied firms have used offensive cyber to track and disrupt movements like BDS.

Finally, Toka contributes to the normalization of offensive cyber as a form of "development." When camera-hacking suites and evidence-erasure tools are funded by the World Bank or IDB as "cyber capacity-building," a political shift is underway, i.e. militarized surveillance becomes part of the standard toolkit of modern governance. The outrage focused on Pegasus obscures firms like Toka, whose activities align more comfortably with Western and multilateral security agendas, and therefore attract less scrutiny. The result is a quiet consolidation of a global surveillance regime in which Israeli-origin technologies are deeply embedded in the security infrastructures of "allied" states, often beyond the reach of public oversight or democratic control.

87 Jessica Buxbaum, "How Israeli Cyber Weapons Are Taking Over Latin America," MintPress News, March 3, 2023, https://www.mintpressnews.com/israeli-cyber-weapons-taking-latin-america/283926/.

88 Kenza Filali, "L'Israélien Illuminant cherche à investir le marché marocain de la cyberdéfense d'État," Le Desk, July 21, 2023, https://mobile.ledesk.ma/enoff/lisraelien-illuminant-cherche-a-investir-le-marche-marocain-de-la-cyberdefense-detat/.

89 AP News, "Garry Kasparov at IMPROVATE Cybersecurity Conference Is Talking About Chess, IA and The Queen's Gambit," AP News (press release), February 16, 2021, https://apnews.com/press-release/pr-newswire/technology-israel-middle-east-garry-kasparov-government-and-politics-e08751ae82db627107fb60602b63062e.

90 Freilich, Charles D, Matthew S Cohen, and Gabi Siboni. 2023. Israel and the Cyber Threat. Oxford University Press.

CORSIGHT AI

Cortica is an Israeli artificial intelligence company spun out of the Technion in 2007.[91] It presents itself as a civilian AI powerhouse, developing "brain-inspired" unsupervised learning and then spinning that core technology into sector-specific companies: a) Autobrains for autonomous driving (backed by BMW and Toyota)[92], b) SeeTrue for automated baggage and security screening[93], c) Fintica for financial analytics, and medical-imaging ventures such as CORDiguide[94]; Finally d) Corsight AI, launched in late 2019, as the facial recognition arm of this portfolio - a "face intelligence" company built to commercialize Cortica's computer-vision capabilities in the field of surveillance.[95]

Cortica is privately held, has raised over $70 million, and operates from Tel Aviv, Haifa, New York, and Geneva.[96] Despite the obvious security applications of its products, it is not listed in SIBAT. This allows Cortica to present itself as a civilian AI firm even as its spin-offs work directly with defense-linked investors and state security agencies.[97] Corsight, for instance, was established as a joint venture between Cortica and the Canadian fund Awz Ventures, which explicitly partners with the Israeli Ministry of Defense R&D directorate and is led by former Mossad, Shin Bet, and other intelligence officials, with former Canadian Prime Minister Stephen Harper as a high-profile advisor.[98]

1. ORIGINS, PERSONNEL, AND POSITION

Corsight AI sits at the junction of Israeli intelligence expertise, academic research, and transnational security capital. It was co-founded by Cortica leadership, CEO Igal Raichelgauz, Dr. Karina Odinaev, and Technion professor Josh Zeevi. Raichelgauz and Odinaev are veterans of elite IDF technological units; Raichelgauz began his career in Unit 8200, Israel's signals intelligence

91 NoCamels Team, "Israeli Startup Raises $5M For Facial Recognition Tech That Can Identify Masked Faces," NoCamels, April 23, 2020, https://nocamels.com/2020/04/israeli-startup-corsight-facial-recognition-tech-masked/.

92 Meir Orbach, "BMW, Toyota Partner With Computer Vision Company Cortica," Calcalist Tech, September 4, 2019, https://www.calcalistech.com/ctech/articles/0,7340,L-3769653,00.html.

93 SeeTrue, "SeeTrue AI Screening Solution Becomes the First and Only to Receive ECAC Certification for Automated Prohibited Items Detection (APIDS)," PR Newswire, January 8, 2026, https://www.prnewswire.com/apac/news-releases/seetrue-ai-screening-solution-becomes-the-first-and-only-to-receive-ecac-certification-for-automated-prohibited-items-detection-apids-302655629.html.

94 Fintica AI, Ltd., "Fintica AI Completes Financial Market Manipulation Detection Pilot for Israel Securities Authority," PR Newswire, September 14, 2021, https://www.prnewswire.com/il/news-releases/fintica-ai-completes-financial-market-manipulation-detection-pilot-for-israel-securities-authority-301376523.html.

95 Corsight AI, "Corsight AI Becomes First Facial Recognition Provider to Achieve ISO/IEC 42001 AI Management Certification," March 25, 2025, https://www.corsight.ai/press/corsight-ai-becomes-first-facial-recognition-provider-to-achieve-iso-iec-42001-ai-management-certification/.

96 Cortica Inc., "Cortica Closes $75 Million in New Funding Round and Acquires Springtide Child Development," PR Newswire, April 18, 2023, https://www.prnewswire.com/news-releases/cortica-closes-75-million-in-new-funding-round-and-acquires-springtide-child-development-301800688.html

97 Rob Watts, "AI in Policing: Doing More with Less," Corsight AI Blog, September 3, 2025, https://www.corsight.ai/facial-intelligence-uk-policing/.

98 Anas Ambri, "Stephen Harper's Firm Behind Spy Tech Used in 'Dystopian' Greek Refugee Camps," Business & Human Rights Resource Centre, January 23, 2025, https://www.business-humanrights.org/en/latest-news/stephen-harpers-firm-behind-spy-tech-used-in-dystopian-greek-refugee-camps/.

and cyber unit.[99] Several Corsight research engineers also come from Unit 8200, carrying over the state's experience in surveillance, interception, and data analysis. Zeevi's academic work underpins Cortica's core algorithms, providing the "brain-inspired" scientific legitimacy.[100] At launch, Corsight was a small team (around 15 staff split between Israel and the US), but it leveraged Cortica's extensive intellectual property, 250+ patents, to claim a deep technical moat.[101]

The company's governance and advisory structure makes its security pedigree explicit. Awz Ventures' founder Yaron Ashkenazi sits on Corsight's board as managing partner; he is a former Shin Bet officer who spent a decade in the VIP protection division.[102] Another board member, Maj. Gen. (res.) Giora Eiland, previously headed the IDF Operations Directorate and later chaired Israel's National Security Council.[103] Early COO Ron Tiberg-Shachar served as an IDF cyber defense officer.[104] This concentration of ex-military and intelligence figures embeds Corsight in the same security ecosystem that governs occupation and regional military operations.

At the same time, Corsight has assembled an international-facing leadership layer designed to make the company acceptable to regulators in Europe and North America. It appointed Tony Porter, the former UK Surveillance Camera Commissioner, as Chief Privacy Officer to oversee "ethical" deployment.[105] This is why Corsight AI, as a firm, speaks two languages at once: internally, the language of state security and military-grade capability; externally, the language of ethics, compliance, and "responsible AI."

2. FROM "FACE INTELLIGENCE" TO POPULATION CONTROL

Corsight develops what it calls "face intelligence" solutions, so facial recognition systems that analyse live or recorded video from cameras to identify individuals at high speed and under non-ideal conditions. Its flagship platform (Fortify) ingests video streams, builds biometric templates from faces, and matches those against watchlists to generate real-time alerts when a person of interest appears or when someone enters a restricted area.[106]

99 Simon Speakman Cordall, "UK Police to Use AI Facial Recognition Tech Linked to Israel's War on Gaza," Al Jazeera, January 28, 2026, https://www.aljazeera.com/news/2026/1/28/uk-police-to-use-ai-facial-recognition-tech-linked-to-israels-war-on-gaza.

100 James Spiro, "Cortica Announces CORDiguide, Medical Spin-Off," Calcalist Tech, March 9, 2021, https://www.calcalistech.com/ctech/articles/0,7340,L-3897691,00.html.

101 Corsight AI, "Corsight AI Announces U.S. Expansion Due to Market Demand for Leading AI Facial Recognition Technology," PR Newswire, March 31, 2022, https://www.prnewswire.com/news-releases/corsight-ai-announces-us-expansion-due-to-market-demand-for-leading-ai-facial-recognition-technology-301514859.html.

102 Awz Ventures, "The Awz Story," accessed April 1, 2026, https://www.awzventures.com/awz-story/.

103 Maj. Gen. (res.) Giora Eiland, "Author Page," Begin-Sadat Center for Strategic Studies, accessed April 1, 2026, https://besacenter.org/author/geiland/.

104 "Ron Tiberg-Shachar," The Org, accessed April 1, 2026, https://theorg.com/org/saiflow/org-chart/ron-tiberg-shachar

105 Biometrics and Surveillance Camera Commissioner, Biometrics and Surveillance Camera Commissioner's Annual Report 2023 to 2024, December 2, 2024, https://www.gov.uk/government/publications/biometrics-and-surveillance-camera-commissioner-report-2023-to-2024/biometrics-and-surveillance-camera-commissioners-annual-report-2023-to-2024-accessible

106 Corsight AI, "Fortify," accessed April 1, 2026, https://www.corsight.ai/product-fortify/.

Technically, the company claims that its algorithms, derived from Cortica's Autonomous AI engine, can recognize individuals even when less than half of the face is visible, when the person is moving, partially obscured, or wearing a mask or helmet. During the COVID-19 pandemic, Corsight aggressively marketed this as a differentiating feature, as it advertised the ability to accurately identify masked individuals, to support quarantine enforcement, and to assist in contact tracing. The same capability is now sold as an advantage in policing, border control, and "safe city" deployments where people may cover their faces or be captured in poor lighting and at sharpangles.[107]

Corsight AI points to independent evaluations, such as a 2020 US Department of Homeland Security facial recognition rally, to show that its system ranked near the top for accuracy, including under mask conditions. [108]Corsight insists, through a paper written by Tony Porter himself, that its models are unbiased across race, gender, and age, addressing the now well-documented discriminatory performance of many facial recognition systems.[109]

From its inception, Corsight worked alongside Israeli military and intelligence agencies, which became early adopters of its systems. The company acknowledges that many deployments are confidential "intelligence agencies and special law enforcement units."[110]

One of the clearest examples is the occupied Palestinian territories. Reports by Amnesty show that Corsight's facial recognition is used by Israeli military intelligence to build and maintain biometric databases of Palestinians.[111] During the War on Gaza, soldiers carried cameras equipped with Corsight software at checkpoints and on evacuation routes, scanning faces of Palestinians without consent and cross-referencing those images against watchlists.[112]

Abroad, the overwhelming majority of deployments are in policing, border control, and critical infrastructure surveillance such as city CCTV networks, airports, mines and banks, border crossings, and public events.[113]

In this sense, Corsight operates as a node in the extension of Israeli security logics beyond territorial boundaries. It expands the reach of Israeli security practices into new jurisdictions, redistributing power toward states and

107 Corsight, "Corsight AI Facial Intelligence in Retail," YouTube video, February 14, 2024, https://www.youtube.com/watch?v=GXDjkwWetpg.

108 James Thorpe, "Corsight AI Receives Top Rankings in 2020 Biometric Technology Rally," Security Journal UK, February 11, 2021, https://securityjournaluk.com/corsight-ai-2020-biometric-technology-rally/.

109 Tony Porter, "Facial Recognition Technology: Blasting the Bias Narrative Out of the Water?," Biometric Technology Today 2022, no. 12 (2022), https://doi.org/10.12968/S0969-4765(22)70622-4.

110 Sheera Frenkel, "Report Reveals Google & Corsight Technologies' Role in Israel's Expansive Facial Recognition Program in Gaza," Business & Human Rights Resource Centre, March 27, 2024, https://www.business-humanrights.org/en/latest-news/report-reveals-google-corsights-technologies-role-in-israels-expansive-facial-recognition-program-in-gaza/.

111 Amnesty International, "Israel/OPT: Israeli Authorities Are Using Facial Recognition Technology to Entrench Apartheid," May 2, 2023, https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/.

112 Nick Robins-Early, "How Israel Uses Facial-Recognition Systems in Gaza and Beyond," The Guardian, April 19, 2024, https://www.theguardian.com/technology/2024/apr/19/idf-facial-recognition-surveillance-palestinians.

113 Corsight AI, "Facial Recognition at Airports," accessed April 1, 2026, https://www.corsight.ai/airports/.

corporate actors that deploy these systems, while positioning individuals and communities elsewhere as targets of the same logics of surveillance, classification, and control.

3. GLOBAL FOOTPRINT

Corsight's expansion maps onto global demand for surveillance infrastructure and mirrors Israel's broader strategy of exporting security technologies as a form of diplomacy, development, and influence-building.[114] The firm reports deployments in over fifty countries, often through local integrators and "safe city" projects that tie together smart lighting, cameras, and analytics.[115]

3.1 SWANA

Awz has spearheaded expansion into Gulf markets opened by the Abraham Accords. Awz established a subsidiary in the UAE to channel Israeli security technologies, including Corsight, into Emirati and regional contracts.[116] Corsight executives have acknowledged talks with Gulf police forces, aligning with broader efforts to position Israel as a premier provider of smart-city and border surveillance to states like the UAE and Saudi Arabia.[117]

3.2 Africa

In Africa, Corsight enters largely through partnerships. In Namibia, Schoemans Technologies became its exclusive distributor, marketing facial recognition systems to government and enterprises.[118] In South Africa, security firm E-Thele integrated Corsight's algorithms into surveillance for mines and banks, monitoring access to high-value sites.[119]

3.3 Asia–Pacific

In the Philippines, the city of Santa Rosa deployed Corsight's platform as part of a "Safe City" initiative, running real-time and forensic scans across its CCTV network to flag wanted persons and identify lost individuals.[120] Corsight has also pursued opportunities in India, where it signed an MoU with Assam's state electronics corporation (AMTRON) to create a Facial Recognition Center of Excellence in Guwahati for Indian government

114 This is well-highlighted in a paper by Lior Tabansky, "Towards a Theory of Cyber Power: The Israeli Experience with Innovation and Strategy," NATO Cooperative Cyber Defence Centre of Excellence, 2018, https://ccdcoe.org/uploads/2018/10/Art-04-Towards-a-Theory-of-Cyber-Power-the-Israeli-Experience-with-Innovation-and-Strategy.pdf.

115 Iain Overton, "Corsight's Crisis: Why British Police Forces Must Rethink Their Israeli Facial Recognition Partners," Action on Armed Violence (AOAV), July 7, 2025, https://aoav.org.uk/2025/corsights-crisis-why-british-police-forces-must-rethink-their-israeli-facial-recognition-partners/.

116 Brigitte Bureau, "Stephen Harper Involved in Company Looking to Arrange Sale of Surveillance Tech to UAE," CBC News, September 29, 2021, https://www.cbc.ca/news/politics/harper-united-arab-emirates-surveillance-technology-1.6192281.

117 "Israelis Pour into UAE for Business and Pleasure," Ynetnews, December 9, 2020, https://www.ynetnews.com/travel/article/Bk00xPYRiD.

118 Corsight AI, "Corsight AI Announces Strategic Partnership With Schoemans Technologies in Namibia," Business Wire, January 30, 2025, https://www.businesswire.com/news/home/20250130146143/en/Corsight-AI-Announces-Strategic-Partnership-With-Schoemans-Technologies-in-Namibia.

119 eThele, "Partners," accessed April 1, 2026, https://www.ethele.co.za/partners/.

120 Corsight AI, "Santa Rosa Safe City Enhances Public Safety with Corsight AI's Unique Facial Intelligence Technology," Business Wire, September 26, 2024, https://www.businesswire.com/news/home/20240926379646/en/Santa-Rosa-Safe-City-Enhances-Public-Safety-with-Corsight-AIs-Unique-Facial-Intelligence-Technology.

clients.[121] A partnership with Singapore-based distributor Netpoleon targets Southeast Asian markets more broadly, combining Corsight's algorithms with local security integrators to insert facial recognition into urban and national security infrastructures.[122]

3.4 Europe

Corsight's presence in Europe runs through airports, hospitals, and policing. It reports deployments in several European airports and healthcare facilities as part of access control and security systems.[123] In the UK, Essex Police adopted a live facial recognition system built with Corsight's technology, using cameras at public events and transit nodes to scan crowds and arrest suspects. Corsight's UK leadership, comprising former policing tech figures, presents these deployments as fully compliant with national regulations, despite civil liberties concerns.[124]

3.5 Americas

Latin America is a key growth region. In Brazil, Corsight partnered with firms like Teltex and Segurimax to roll out facial recognition hubs across Sao Paulo state police battalions.[125] Israeli smart lighting company Juganu integrated Corsight's system into "smart" lampposts on the Friendship Bridge between Brazil and Paraguay, capturing faces and license plates of travellers and streaming that data to border authorities, an example of biometric surveillance woven into infrastructure that appears neutral (lighting) but functions as a data collection node.[126] In Paraguay, Grupo Vázquez licensed Corsight algorithms to embed facial recognition across its diversified businesses and to sell services to government agencies.[127]

In Mexico, Corsight partnered with security firm ISEG to install facial recognition at three hospitals in Monterrey (Auna healthcare network), monitoring ICU and other critical areas.[128] Corsight has also been linked to Mexican federal police and other regional agencies.[129] In Colombia, Bogotá's metropolitan police ran a pilot in 2023 using Corsight to identify suspects from CCTV footage. Across the Americas, the pattern is consistent: integration

121 "Corsight AI Partners for Facial Recognition Projects in India," Biometric Update, August 19, 2021, https://www.biometricupdate.com/202108/corsight-ai-partners-for-facial-recognition-projects-in-india.

122 Corsight AI, "Leading Facial Recognition Technology Provider, Corsight AI, Announces Netpoleon as Distribution Partner for Asia," PR Newswire, May 12, 2021, https://www.netpoleons.com/news/leading-facial-recognition-technology-provider-corsight-ai-announces-netpoleon-as-distribution-partner-for-asia.

123 "EU AI Pact Sets New Standards for Ethical AI Use Across Europe," Biometric Update, September 13, 2024, https://www.biometricupdate.com/202409/eu-ai-pact-sets-new-standards-for-ethical-ai-use-across-europe

124 Robert Booth, and Mark Wilding. "Essex Police Pause Facial Recognition Camera Use After Study Finds Racial Bias." The Guardian, March 19, 2026. https://www.theguardian.com/technology/2026/mar/19/essex-police-pause-facial-recognition-camera-use-study-racial-bias

125 Corsight AI. "Corsight AI Partners with Segdboa to Provide São Paulo Military Police with Facial Intelligence Capabilities." Business Wire, June 19, 2024. https://www.businesswire.com/news/home/20240619024171/en/Corsight-AI-Partners-with-Segdboa-to-Provide-So-Paulo-Military-Police-with-Facial-Intelligence-Capabilities.

126 Techtime. "Juganu Made the Brazil-Paraguay Border Safer." Techtime, July 2, 2020. https://techtime.news/tag/smart-city/.

127 Business Wire. "Corsight AI Partners with ITTI from Grupo Vázquez to Enhance Security, Efficiency, and User Experience with Facial Intelligence." Financial Post, September 2, 2024. https://financialpost.com/pmn/business-wire-news-releases-pmn/corsight-ai-partners-with-itti-from-grupo-vazquez-to-enhance-security-efficiency-and-user-experience-with-facial-intelligence.

128 Corsight AI. "Corsight AI Partners with ITTI from Grupo Vázquez to Enhance Security, Efficiency, and User Experience with Facial Intelligence." Security Journal Americas, September 2024. https://securityjournalamericas.com/partnership-for-facial-intergration/

129 Ibid.

into policing, border control, hospitals, and high-value commercial sites, under the banner of modernization and efficiency.[130]

Corsight's expansion is driven by an advertising strategy that combines elite security credentials with ethical rhetoric. The company highlights its "military-grade" performance and Unit 8200 lineage when selling to security services, while stressing ethics, privacy compliance, and the presence of a former UK surveillance regulator when addressing publics and regulators in liberal democracies.[131] Despite these deep institutional ties to the IDF, Corsight's CEO has publicly emphasized that the company "does not sell to China, Russia or Myanmar because of human rights and ethics," presenting its technology as "a force for good" in law enforcement.[132] Such claims position the firm within a selective ethical framework, where the legitimacy of surveillance is not questioned in itself but is instead reframed through the choice of clients, allowing the technology to be marketed as responsible and rights-conscious, even as it remains embedded in infrastructures of militarized control.

KEY TAKEAWAYS

The significance of these findings lies not only in what these firms do, but in the infrastructure that makes their operations possible. The findings of this paper demonstrate that Toka and Corsight AI are not best understood as isolated private technology companies, but as firm-level vehicles through which Israeli militarized industrial policy is quite literally laundered.133 This aligns with a growing body of scholarship that conceptualizes surveillance as emerging from the intersection of state power,134 corporate actors,135 and transnational markets136 rather than from discrete institutional domains.

While Toka and Corsight operate in distinct technological domains, they perform complementary roles within the same industrial policy architecture. Toka exemplifies how offensive cyber capabilities are integrated into governance through the language of lawful intelligence and resilience, while Corsight demonstrates how biometric surveillance is normalized through discourses of ethical AI and compliance. Building on recent work by the AI Now Institute on "AI nationalisms," which highlights how states mobilize industrial policy to structure AI ecosystems in line with geopolitical and

130 IFSEC Insider. "Bogotá Police Using Facial Recognition to Enable Arrest of Murder and Theft Suspects." IFSEC Global, November 8, 2023. https://www.ifsecglobal.com/video-surveillance/bogota-police-using-facial-recognition-to-enable-arrest-of-murder-and-theft-suspects/

131 Liberty. "Liberty Responds to Essex Police Pausing Use of Facial Recognition Cameras Due to Racial Bias." Liberty Human Rights, March 20, 2026. https://www.libertyhumanrights.org.uk/issue/liberty-responds-to-essex-police-pausing-use-of-facial-recognition-cameras-due-to-racial-bias/

132 Cheslow, Daniella. "Israeli Firm Develops Body Cams with Facial Recognition Technology." The Times of Israel, January 23, 2022. Updated January 25, 2022. https://www.timesofisrael.com/israeli-firm-develops-body-cams-with-facial-recognition-technology/.

133 Yaron Salman, "Light unto the Nations Through Arms Sales: Israel's Arms Diplomacy Goals, Achievements, and Limitations," Contemporary Review of the Middle East 12, no. 2 (2025), https://doi.org/10.1177/23477989251318874.

134 Feldstein, Steven. "Front Matter." In The Global Expansion of AI Surveillance. Washington, DC: Carnegie Endowment for International Peace, 2019. http://www.jstor.org/stable/resrep20995.1.

135 7amleh – The Arab Center for the Advancement of Social Media. Israel's Surveillance Industry and Human Rights: Impact on Palestinians and Worldwide. December 2023. https://7amleh.org/storage/Israel%E2%80%99s%20Surveillance%20Industry%20english4.pdf

136 Ahmad H. Sa'di, "Israel's Settler-Colonialism as a Global Security Paradigm," Race & Class 63, no. 2 (2021): 21–37, https://doi.org/10.1177/0306396821996231.

economic priorities137, Israel's AI industrial policy can be understood as an intensified formation in which AI development is explicitly organized around militarization and security imperatives.[138]

The findings also show the normalization of surveillance, which scholars have used described as technocratic discourse.[139] Both firms use terminologies of public safety, cyber resilience, lawful intelligence, and ethical AI as legitimizing frameworks rather than neutral descriptors. On a material level, the findings show that the firm form is central to the transnationalization of militarized technologies.[139] Firms such as Toka and Corsight do not simply commercialize state innovations; they organize, mediate, and diffuse them through complex contractual and organizational arrangements. This supports and extends arguments about the emergence of an "intelligence-industrial complex," in which corporate actors are structurally embedded in state security infrastructures.[140]

Echoing critiques of "ethical AI" as a form of governance without constraint[141], the findings indicate that ethical claims function as mechanisms of market differentiation rather than substantive limitations. Finally, the findings reinforce longstanding critiques of the erosion of boundaries between state and market in security production.[142]

The World Bank and the Inter-American Development Bank have, over the past decade, financed cybersecurity and digital governance programs that have enabled the integration of Israeli surveillance firms into state infrastructures across the Global South and beyond. Between 2020 and 2023, contracts in Nigeria, Moldova, Ghana, and Chile were awarded to Toka Group. In parallel, Corsight AI has embedded its systems across policing, border control, and urban surveillance infrastructures in 50+ countries.

First, firms such as Toka and Corsight are not conventional private-sector actors operating at the margins of the state. They are organizational extensions of a broader militarized industrial policy, translating military and intelligence capabilities into scalable products for global markets. Corsight AI operates through a parallel logic. Emerging from a network of military-trained engineers and intelligence-linked governance structures, it develops facial recognition systems capable of identifying individuals under conditions of occlusion, movement, and low visibility.

137 Amba Kak, AI Nationalism(s): Global Industrial Policy Approaches to AI—Executive Summary (New York: AI Now Institute, 2024), https://ainowinstitute.org/publications/ai-nationalisms-executive-summary.

138 Anthony King, "Digital Targeting: Artificial Intelligence, Data, and Military Intelligence," Journal of Global Security Studies 9, no. 2 (June 2024): ogae009, https://doi.org/10.1093/jogss/ogae009.

139 Rita Abrahamsen and Michael C. Williams, "Securing the City: Private Security Companies and Non-State Authority in Global Governance," International Relations 21, no. 2 (2007): 237–253, https://doi.org/10.1177/0047117807077006.

140 This paper has drawn on and referenced multiple works by Sophia Goodfriend, building on them to develop its argument. See: Sophia Goodfriend, "New Tech, Old War," London Review of Books (blog), July 2023, https://www.lrb.co.uk/blog/2023/july/new-tech-old-war

141 Jacob Metcalf, Emanuel Moss, and danah boyd, "Owning Ethics: Corporate Logics, Silicon Valley, and the Institutionalization of Ethics," Social Research: An International Quarterly 82, no. 2 (Summer 2019): 449–476 (New York: Data & Society Research Institute), https://datasociety.net/wp-content/uploads/2019/09/Owning-Ethics-PDF-version-2.pdf.

142 Linda Weiss and Elizabeth Thurbon, "Power Paradox: How the Extension of US Infrastructural Power Abroad Diminishes State Capacity at Home," Review of International Political Economy 25, no. 6 (2018): 779–810, https://doi.org/10.1080/09692290.2018.1486875.

Second, the global expansion of these technologies is enabled by the firm form itself, which operates as a core instrument of industrial policy. Through subsidiaries, joint ventures, licensing agreements, and local intermediaries, these actors move across jurisdictions while fragmenting accountability. This organizational flexibility is not incidental; it reflects a mode of industrial organization in which state priorities are diffused through firms that can reconfigure their legal, financial, and operational structures in response to regulatory environments. In this sense, the firm becomes the mechanism through which militarized industrial policy is enacted beyond the state's formal boundaries. It allows access to markets and enables the circumvention of constraints that would otherwise apply to direct state action. What emerges is not a linear export model, but a distributed infrastructure through which surveillance capabilities are routed, reassembled, and embedded within civilian governance systems.

Third, multilateral development institutions function as critical interfaces in this process. By incorporating such firms into programs framed as digital capacity-building, cyber resilience, or institutional modernization, these institutions facilitate the normalization of surveillance technologies as components of legitimate governance. In doing so, they do not merely fund technological adoption; they actively participate in the construction of new markets for militarized technologies, recasting them as neutral, necessary, and developmental

FROM SETTLER COLONIALISM AND THE REMOTE-CONTROL OCCUPATION: **TECH-INNOVATION, NEOLIBERAL ZIONISM, AND DIGITAL SUMŪD IN TIMES OF GENOCIDE**

AREES BISHARA

Introduction	37
Literature Review	39
Methodology	42
Findings and discussion	43
Conclusion	56

Arees is a research fellow at the Department of Political Science and Sociology, Scuola Normale Superiore di Pisa. She is a scholar of political and organizational sociology whose work bridges Israel/Palestine studies, technology, gender, and settler colonialism. She has held research positions at Tel Aviv University, Michigan State University, and the European University Institute, among others.

Arees' research project, Censuring Palestine: Unveiling the Hypocrisy and Dehumanization across Power Structures in Times of Genocide, investigates how governments, corporations, and academia perpetuate censorship and dehumanization of Palestine, particularly through technological and institutional power.



ABSTRACT

This article theorizes how the convergence of technological innovation and military strategy has reconfigured the Israeli occupation into digital settler colonialism, intensified after October 7, 2023. Extending digital colonialism debates, the study shows Israel's innovation economy operates as both national project and global business model, embedding the tech sector in genocidal violence. Grounded in settler-colonial studies, digital colonialism theory, Foucauldian biopolitics, and Bauman's analysis of institutional violence, it conceptualizes a remote-control occupation produced through the military–academic–tech nexus under neoliberal Zionism. Drawing on thematic content analysis and interviews with Palestinian technologists (2020–2024), the article identifies three modalities of digital elimination: physical (AI-assisted targeting), economic (military R&D in global markets), and epistemic (digital censorship). Consequently, Palestinians cultivate digital sumūd—networked practices of endurance and resistance.

Keywords: **Digital settler colonialism; neoliberal Zionism; digital sumūd; futurity.**

1. INTRODUCTION

Since the 2000s, scholars have framed the Israeli occupation as a paradigmatic form of settler-colonial governance structured around the logic of elimination (Lentin, 2020; Sabbagh-Khoury, 2022; Sa'di, 2021; Veracini, 2011, 2015; Wolfe, 2006). In Palestine, what historically relied on territorial seizure, military checkpoints, and demographic regulation increasingly operates through remote-control infrastructures, predictive analytics, biometric databases, and AI-assisted targeting. Across Gaza, the West Bank, and historic Palestine, military, academic, and corporate actors collaborate to refine new regimes of algorithmic violence and population management (Ahmad, 2021; Avis et al., 2025; Bevilacqua, 2022; Musleh, 2018; Sa'di, 2021; Shalhoub-Kevorkian, 2015, 2017; Shehadeh, 2023; Tawil-Souri, 2012; Zureik, 2016b, 2020; Zureik et al., 2010).

This transformation intensified after October 7, 2023. The ongoing genocidal assault on Gaza coincided with the expanded use of automated kill lists, facial-recognition systems, and machine-assisted aerial warfare. Israeli officers described an AI-driven "broad hunt," where homes are destroyed on the basis of a single individual's presence. This reflects Bauman's (Bauman, 1989) account of institutional violence: bureaucratized harm that distances actors from consequences."

These systems have expanded well beyond Israel's borders. The shift from the celebrated "Start-Up Nation" (Senor & Singer, 2009) toward what might be termed an "exit nation" was enabled not by market liberalization alone but by deliberate state coordination. Maggor (Maggor, 2020) shows that Israel's innovation economy emerged through a neo-developmental model in which the state directed capital and cultivated high-tech capacity to integrate firms into global markets. This fusion of militarism and innovation

is conceptualized here as neoliberal Zionism (Getzoff, 2020): a formation that blends nationalist security doctrine with market rationality and technological optimism, framing "tech as practical Zionism." according to Gilad Rabinovich's statement.[1]

These developments are not merely military innovations but products of a broader political economy. Israeli technology elites increasingly act not only as beneficiaries of state policy but as political actors shaping it. As Shihadeh (Shihadeh, 2024) argues, the high-tech sector has shifted from indirect influence to direct institutional power-building, consolidating techno-political authority domestically while deepening global entanglements. Through arms transfers, cybersecurity contracts, AI partnerships, and venture-capital flows, Israeli tech actors bind multinational corporations and foreign governments to Israel's security-innovation ecosystem (Loewenstein, 2023; Swed & Butler, 2015; Tariq, 2024; Tarvainen & Challand, 2024).

These international entanglements render foreign governments and private firms structurally complicit in the infrastructures of occupation. Albanese's (2025)[2] report, **From the Economy of Occupation to the Economy of Genocide**, demonstrates how corporate systems profit from and enable displacement, apartheid, and genocide, including through dual-use technologies such as biometric surveillance, AI targeting tools, and cloud-based military platforms that turn occupied territory into a testing ground.

Following Albanese (2025)[3] and Helga Tawil-Souri's (Tawil-Souri, 2012) who theorizes Gaza as a "high-tech enclosure," this article situates contemporary Israeli domination within a broader theorization of digital settler colonialism. Gaza exemplifies a space where physical siege converges with digital, biometric, and infrastructural control, rendering the territory simultaneously isolated, monitored, and technologically dependent. Drawing on settler-colonial studies (Lentin, 2020; Sabbagh-Khoury, 2022; Sa'di, 2021; Veracini, 2011, 2015; Wolfe, 2006), digital colonialism scholarship (Bevilacqua, 2022; Couldry & Mejias, 2019; Kwet, 2019, 2022), and informed by Foucauldian biopolitics (Foucault, 2008) and Bauman's insights on institutional violence (Bauman, 1989), this article advances two core arguments.

First, the occupation has entered a digitally mediated phase in which settler-colonial logics extend into algorithmic governance. Under neoliberal Zionism, technological innovation legitimizes and scales violence while embedding the occupation within global AI and security markets. The civil–military–academic nexus co-produces surveillance systems that render Palestinian life hyper-visible to machines while erasing political agency.

Second, Palestinians enact **digital sumūd**, a set of resilient techno-practices that refuse erasure and assert collective presence. Activists, technologists,

1 Gilad Rabinovich is a tech investor in the Israeli High tech.

2 Albanese, F. (2025). From the economy of occupation to the economy of genocide: Report of the UN Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967. Office of the UN High Commissioner for Human Rights. https://www.un.org/unispal/document/

3 Albanese, F. (2025). From the economy of occupation to the economy of genocide: Report of the UN Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967. Office of the UN High Commissioner for Human Rights. https://www.un.org/unispal/document/

and civil-society collectives cultivate counter-infrastructures—archival platforms, mesh networks, and transnational digital campaigns—that sustain political agency amid surveillance, disconnection, and violence. While Israeli institutions deploy algorithmic systems to fragment and silence Palestinian presence, Palestinians repurpose digital tools to endure, document, and remain connected.

Accordingly, this study addresses two central questions: (1) How does Israel's innovation economy—intertwined with military and academic institutions—operationalize digital settler colonialism amid ongoing genocide? (2) How do Palestinians enact digital sumūd to resist, subvert, and re-signify technologies designed to physically eliminate, dehumanize, and censor them? In addressing these questions, the article contributes to scholarship on technology and innovation, settler colonialism, and Palestinian sumūd by situating digital infrastructures within global hierarchies of power and resistance.

2. LITERATURE REVIEW

2.1 SETTLER COLONIALISM IN THE DIGITAL AGE: ALGORITHMIC GOVERNANCE, BIOPOLITICS, AND PHYSICAL ELIMINATION

Settler-colonial theory posits the "logic of elimination" as the core structure for removing Indigenous populations and replacing them with a new political order (Wolfe, 2006 ; Veracini, 2011, 2015; Sabbagh-Khoury, 2022). In Palestine, this logic has long manifested as land confiscation and racialized surveillance (Ahmad, 2021; Shalhoub-Kevorkian, 2015; Zureik, 2001, 2016b, 2016a; Zureik et al., 2010).

Over the last two decades, this structure has undergone a digital transformation where mechanisms of physical control (checkpoints, patrols) are supplemented or replaced by algorithmic governance—biometric databases, predictive analytics, and automated targeting systems (Loewenstein, 2023; Musleh, 2018; Zureik, 2001, 2016b; Zureik et al., 2010).

This shift must be viewed through a biopolitical lens (Foucault, 2008), where digital-settler colonialism is conceptualized as the fusion of settler domination with computational infrastructures. Algorithmic governance extends settler sovereignty into computational forms that manage, classify, and target Palestinian bodies, translating elimination into computational code. Importantly, this process facilitates "institutional violence" (Bauman, 1989), where the removal of human agency through automated systems creates moral distance, reducing victims to data points and enabling the mechanical execution of violence. Parallel scholarship on digital colonialism emphasizes that these infrastructures intensify, rather than replace, traditional domination circuits , (Gillespie, 2018, 2018; Kwet, 2019, 2022; Noble, 2018, 2018; Tarvainen & Challand, 2024) reproducing longstanding histories of racialization and economic subjugation under neoliberal ideologies (Clarno, 2018b, 2018a; Johnson, 2019; Lloyd & Wolfe, 2016; Wildeman, 2019).

2.2 NEOLIBERAL ZIONISM AND THE POLITICAL ECONOMY OF TECHNOLOGICAL INNOVATION

The perpetuation of digital-settler colonialism is sustained by an integrated political economy. The Israeli high-tech sector, often promoted under the "start-up nation" narrative (Senor & Singer, 2009), was strategically built through coordinated state investment, military R&D, and venture capital (Maggor, 2020). This produced a powerful civil–military–academic complex where military units (e.g., Unit 8200) function as incubators, converting military surveillance tools into commercial products often tested on Palestinians and marketed as "field-proven" (Loewenstein, 2023; Swed & Butler, 2015; Wind, 2024). This formation is defined as neoliberal Zionism (Getzoff, 2020), which fuses security doctrine with market rationality, reframing technological innovation as national service—"tech as practical Zionism". This economic engine produces structural dependency for Palestinians, who are positioned as surveilled, subcontracted labor under the rhetoric of "economic peace building" (Last, 2007). This political economy is increasingly globalized through multinational partnerships, embedding corporate firms within occupation infrastructures. The same complex that governs economic dependency also governs knowledge production, creating conditions for the second and third modes of elimination.

2.3 EPISTEMOLOGY, ARCHIVES AND THE REPRODUCTION OF KNOWLEDGE

The economic and biopolitical systems outlined above are maintained by an epistemic infrastructure that legitimizes domination. Epistemological violence (Fanon, 1963) is resisted through epistemic (Mignolo, 2009, 2011; Mignolo & Walsh, 2018). In the Israeli context, academic and media institutions function as militarized knowledge regimes (Wind, 2024), enforcing an epistemic hierarchy that privileges Zionist narratives while marginalizing or criminalizing Palestinian history (Peled-Elhanan, 2012; Sabbah-Karkabi & Abu-Rabia-Queder, 2025). This elimination is amplified by global celebratory narratives (Senor & Singer, 2009) that sacralize Israeli technological progress, obscuring colonial conditions.[4]

Furthermore, epistemic domination manifests through archival control. While Israel has historically confiscated and destroyed physical Palestinian cultural artifacts since the Nakba (Amit, 2011; Masalha, 2012; Sela, 2018), the current genocide has escalated this into a systematic digital data-cide. The targeting of universities and servers in Gaza—defined as scholasticide (Giroux, 2025)—represents the cutting edge of digital settler colonialism. This is not merely about destroying buildings; it is an attempt to erase the "digital twin" of Palestinian society by deleting cloud-based archives, academic records, and digital memories. Coupled with algorithmic governance and platform censorship, this results in epistemic digital elimination:

4 See Books such as Let There Be Water (Siegel M., 2015), and Thou Shalt Innovate (Jorisch, 2018) frame Israeli technological development as a civilizational mission to "make the desert bloom" or "repair the world," sacralizing innovation as moral virtue while erasing the colonial conditions that enable it. These narratives present technological progress as evidence of national genius and divine favor, thereby legitimizing Israel's global techno-political authority and obscuring Palestinian dispossession. In this configuration, tech discourse itself functions as a **mode of epistemic reproduction**, stabilizing Zionist myths and marginalizing Palestinians as either absent, irrelevant, or "politicized."

a remote-controlled process that renders Palestinian life unsearchable and invisible, ensuring that the destruction of the physical body is followed by the automated erasure of its history and future from the global digital record.

2.4 DIGITAL REPRESSION, SUMŪD AND DECOLONIALIZATION

Digital repression complements traditional state control through online speech restriction, communication monitoring, and surveillance, alongside physical imprisonment and censorship (Awwad & Toyama, 2024). Within this context, Israel's techno-colonial regime extends longstanding systems of domination into the digital sphere. Yet Palestinian digital practices demonstrate how online spaces function as arenas of activism, resistance and professional mobility (Althalathini & Tlaiss, 2023; Aouragh, 2011; Tawil-Souri & Aouragh, 2014; York, 2012). Digital activism creates participatory possibilities by enabling autonomous, transnational, and collective participation (Awwad & Toyama, 2024) and technological engagement can function as a form of agency (Rindova et al., 2009).

These possibilities coexist with constraints such as unequal access, echo chambers, and vulnerability to surveillance. Digital repression intensifies these limits through platform governance, algorithmic control, and the erasure of cultural infrastructures (Awwad & Toyama, 2024). These dynamics constitute **epistemic digital elimination**—the systematic devaluation of Palestinian knowledge.

Studies further highlight content moderation, algorithmic ranking, and automated classification function as epistemic infrastructures that determine what is visible, credible, or shareable (Peeters & Schuilenburg, 2023). In the Palestinian case, civil-society research demonstrates a pattern of algorithmic epistemic asymmetry: Palestinian content is disproportionately restricted, while incitement against Palestinians persists largely unchallenged (7amleh, 2024; Ahmad, 2021; Al-Salhi, 2021).

Research on Palestine distinguishes between activism aimed at expanding digital access and activism that uses digital platforms for political goals. The latter—often described as a "cyber intifada" (Aouragh, 2011; Tawil-Souri & Aouragh, 2014) —includes circulating testimonies, documenting violence, and advancing global campaigns such as the Boycott, Divestment, and Sanctions movement. Hashtags like #GazaUnderAttack have become key tools for real-time witnessing and transnational advocacy.

These practices intersect with **sumūd**, historically denoting steadfast refusal to relinquish land or identity (Abu-Lughod, 2020; Busse, 2022; Hammami, 2005; Rijke & Van Teeffelen, 2014; Tatour, 2019). Digitally, sumūd entails resisting erasure and countering algorithmic repression (Khoury-Machool, 2007; Shehadeh, 2023). Projects like Visualizing Palestine, Palestine Open Maps, and the Encyclopedia of the Palestine Question rebuild suppressed histories, while organizations such as 7amleh contest censorship—forms of **epistemic sovereignty**.

Digital sumūd also operates as epistemic disobedience aligned with decolonial design principles (Mignolo, 2009, 2011; Mignolo & Walsh, 2018) and resonates with global critiques of data colonialism (Couldry & Mejias, 2019; Milan & Treré, 2019). Concepts such as Shehadeh's "digital floating homeland" (Shehadeh, 2023) and Khoury-Machool's "electronic resistance" (Khoury-Machool, 2007) capture how Palestinians create shared digital spaces across fragmented geographies. After October 7, 2023, these practices intensified as testimonies circulated despite blackouts and algorithmic suppression, transforming surveillance systems into infrastructures of witnessing and mobilization (Aouragh, 2011; Khoury-Machool, 2007).

3. METHODOLOGY

This study employs a qualitative mixed methods design to address the dual research questions of digital settler colonialism and digital sumūd. Grounded in decolonial research methodologies, the analysis treats AI systems and data-governance regimes as sociotechnical assemblages shaped by militarism and logics of elimination.

3.1 RESEARCH DESIGN AND DATA

This study integrates two complementary approaches:

- One: thematic discourse and content analysis of investigative reports and media coverage (2020–2025) across five categories (AI-targeting, censorship, academic complicity, and digital sumūd) (See the full report **here**). A curated archive of publicly available social media posts by Gazans (October 2023–February 2024) was also analyzed to understand lived experiences of digital warfare.
- Two: semi-Structured Interview with fifteen Palestinian technologists (selected from a dataset of seventy conducted 2020–2024) from Gaza, the West Bank/East Jerusalem, and the 1948 territories. Snowball sampling was used, and interviews were conducted in Arabic. Strict anonymity protections were maintained.

This design offers a multilayered account of how digital infrastructures sustain settler-colonial power while documenting digital sumūd.

3.2 ANALYTICAL PROCEDURES

Data were gathered and coded and synthesized into thematic categories using ATLAS.ti. Analysis focused on the convergence of military, private-tech, and academic institutions, and on discursive mechanisms that depoliticize technology while producing silencing and dehumanization. Coding combined deductive strategies (scholarly concepts) and inductive approaches. Interviews were analyzed through narrative strategies to identify junctures where technologists accommodate, resist, and transform constraints within the settler-colonial technological landscape

4. FINDINGS AND DISCUSSION

The findings of this study show that the Israeli occupation has evolved into a paradigmatic form of digital settler colonialism. In this configuration, algorithmic systems, digital infrastructures, and innovation economies do not replace traditional military or bureaucratic functions; rather, they function as an augmented layer of colonial power that accelerates and scales surveillance, control, and elimination processes. Consequently, the occupation increasingly operates through AI-driven targeting, biometric surveillance, and networked control—illustrating the convergence of technological modernity and colonial domination. Extending Wolfe's (Wolfe, 2006) argument, this study demonstrates that the "logic of elimination" unfolds simultaneously across spatial and digital frontiers. Within this regime, Palestinians become hyper-visible as data subjects yet politically invisible—a paradox reflecting an automated apartheid where racialized control is translated into computational form. Algorithmic systems governing movement, access, and visibility embed the logic of elimination directly into digital infrastructures. This exposes the limits of "ethical" AI discourse; here AI functions as a lethal extension of settler power, where "precision" masks state violence. The following analysis examines three modalities of digital elimination—physical, economic, and epistemic—and explores how Palestinians enact digital sumūd to resist and subvert these technologies of control.

4.1 THREE MODALITIES OF ELIMINATION

4.1.1 Physical Elimination: Algorithmic Targeting, AI-Assisted Warfare, Surveillance, and Remote-control Occupation

This section extends settler-colonial and digital-colonial frameworks by showing how biometric surveillance and AI-targeting translate the logic of elimination into computational systems. Systems like Blue Wolf, Red Wolf, and Wolf Pack create an integrated surveillance regime across the oPt, which Amnesty International calls "automated apartheid," institutionalizing racial segregation.[5]

Blue Wolf software[6][7][8], allows soldiers to photograph Palestinians and instantly cross-check biometric databases. The app features a "leaderboard" rewarding military units with rewards like paid time away for capturing the most faces.[9][10] Amnesty warned Palestinians face "the risk of an algorithm

5 Amnesty International. (2023). Automated apartheid: Israel's use of facial recognition technology in the Occupied Palestinian Territories. https://www.amnesty.org/en/documents/mde15/6701/2023/en/

6 Middle East Eye. (2021, March 18). Israel: what's the Blue Wolf app? Soldiers use it to photograph Palestinians. Middle East Eye. https://www.middleeasteye.net/news/israel-whats-blue-wolf-app-soldiers-use-photograph-palestinians

7 Haaretz. (2023, May 2). Israel using facial-recognition tech to entrench apartheid, Amnesty Intl says. Haaretz. https://www.haaretz.com/israel-news/2023-05-02/ty-article/highlight/israel-using-facial-recognition-tech-to-entrench-apartheid-amnesty-intl-says/00000187-db8a-d9b4-abaf-fbbe6c080000

8 The Guardian. (2024, April 19). How Israel uses facial-recognition systems in Gaza and beyond. The Guardian. https://www.theguardian.com/technology/2024/apr/19/idf-facial-recognition-surveillance-palestinians

9 The Guardian. (2024, April 19). How Israel uses facial-recognition systems in Gaza and beyond. The Guardian. https://www.theguardian.com/technology/2024/apr/19/idf-facial-recognition-surveillance-palestinians

10 Middle East Eye. (2021, November 9). Meet Blue Wolf, the app Israel uses to spy on Palestinians in the occupied West Bank. Middle East Eye. https://www.middleeasteye.net/news/israel-whats-blue-wolf-app-soldiers-use-photograph-palestinians

tracking them or preventing entry to their neighborhoods."[11] Red Wolf, operating at Hebron checkpoints, determines passage and automatically enrolls Palestinians into databases without consent. A resident noted that soldiers can bar entry to their own home by claiming a person is "not in the database".[12]

These technologies exemplify Foucault's (Foucault, 2008) epistemic infrastructures, where colonial power is embedded in code. A 7amleh report concludes this deepens insecurity and militarization under the guise of security.[13] As Tawil-Souri (Tawil-Souri, 2012) argues, Palestinian spaces function as "high-tech enclosures," reflecting the bureaucratic and technological order which mediate the colonial violence. Additionally, AI-assisted targeting systems extend this logic by transforming Palestine into a laboratory for computational warfare. As Avner Ben Zaken, head of the Israeli army's Technology and Logistics Division, explained:

"If I am developing a product and want to test it in the field, all I need to do is go five or ten kilometers… Gaza Is considered a site for testing forms of unmanned combat." (Musleh, 2018).

This corresponds with research showing that Israel's innovation economy is intertwined with military field-testing and the export of dual-use technologies (Kwet, 2022; Tarvainen & Challand, 2024).

Several reports[14][15][16] document systems such as **Lavender**, **Where's Daddy?** and **The Gospel**. Developed by Unit 8200, these systems flagged tens of thousands of Palestinians as targets with minimal human oversight. One officer described feeding hundreds of names into the system, calling them "garbage targets," and bombing individuals once located at home." [17]

Parallel reporting describes a "ChatGPT-like" LLM automating threat analysis and generating arrest lists[18]. As Nadim Nashif stated, "Palestinians have become subjects in Israel's laboratory".[19] These systems blur distinc-

11 Amnesty International. (2023, May 2). Israel/OPT: Israeli authorities are using facial-recognition technology to entrench apartheid. Amnesty International. https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/

12 Amnesty International. (2023, May 2). Israel/OPT: Israeli authorities are using facial-recognition technology to entrench apartheid. Amnesty International. https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/

13 7amleh. (2023, December 19). Israel's surveillance industry and human rights: Impact on Palestinians and worldwide. 7amleh. https://7amleh.org/post/7amleh-center-issues-a-report-on-israel-s-surveillance-industry-and-its-impact-on-human-rights

14 +972 Magazine. (2024, April 3). Lavender AI: How the Israeli army is using artificial-intelligence tools in Gaza. +972 Magazine. https://www.972mag.com/lavender-ai-israeli-army-gaza/

15 The Guardian. (2024, April 3). 'The machine did it coldly': Israel used AI to identify 37,000 Hamas targets. The Guardian. https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes

16 Albanese, F. (2025). From economy of occupation to economy of genocide: Report of the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967. United Nations. https://www.un.org/unispal/document/a-hrc-59-23-from-economy-of-occupation-to-economy-of-genocide-report-special-rapporteur-francesca-albanese-palestine-2025/

17 +972 Magazine. (2024, April 3). Lavender AI: How the Israeli army is using artificial-intelligence tools in Gaza. +972 Magazine. https://www.972mag.com/lavender-ai-israeli-army-gaza/

18 +972 Magazine. (2025, March 6). Israel developing ChatGPT-like tool that weaponizes surveillance of Palestinians. +972 Magazine. https://www.972mag.com/israeli-intelligence-chatgpt-8200-surveillance-ai/

19 +972 Magazine. (2025, March 6). Israel developing ChatGPT-like tool that weaponizes surveillance of Palestinians. +972 Magazine. https://www.972mag.com/israeli-intelligence-chatgpt-8200-surveillance-ai/

tions between civilians and combatants and enable "wide-area hunting." Such systems exemplify Bauman's (Bauman, 1989) notion of institutional violence, where killing becomes procedural and morally distanced.

4.1.2 Economic elimination: Tech sector, academia, and military complex

This section analyzes the "economy of occupation"—and its recent escalation into what Albanese (Albanese, 2025) terms an "economy of genocide"—through the lens of neoliberal Zionism. This ideological project merges the high-tech sector, military apparatus, and academic institutions to entrench a settler-colonial order characterized by territorial consolidation and digital labor exploitation.

Civil–Military–Academic Pipeline

In this regime, Israeli universities and private technology corporations are not merely adjacent to the state; they are structurally integrated hubs where weapons and surveillance systems are developed, field-tested on Palestinian populations, and subsequently commercialized for the global market. Albanese(Albanese, 2025)[20] argues these institutions "have enabled the conditions for the elimination of Palestinians" by providing technical foundations for state violence.

Israeli Universities host R&D collaborations with arms firms (Elbit Systems, Rafael) serving as recruitment pipelines for military intelligence units. Marwa, Palestinian engineers feel like "stranger, doesn't belong" at university job fairs dominated by military contractors - a sentiment echoed by activists who describe the university as a "partner in Israel's mechanisms of occupation".[21]

Beyond recruitment, these institutions play a direct operational role in warfare. Multiple Reports[22][23][24] showed direct universities' role in weapons development, the formulation of doctrines like the Dahiya Doctrine, and wartime initiatives such as TAU's "engineering war room" (See the **video**) and the University of Haifa's propaganda campaigns and material support for soldiers.[25] As Maya Wind (Wind, 2024) shows, these institutions also suppress Palestinian academic rights while reinforcing apartheid structures. Palestinian students in the Israeli Academia have told Middle East Eye[26] they feel increasingly isolated on campus.

20 Albanese, F. (2025). From the economy of occupation to the economy of genocide: Report of the UN Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967. Office of the UN High Commissioner for Human Rights. https://www.un.org/unispal/document/

21 Kogan, Y. (2022, April 7). Academia, weapons and occupation: How Tel Aviv University serves the interests of the army and the military-industrial complex [In Hebrew]. Zo HaDerekh. https://zoha.org.il/111858/

22 BDS Movement. (n.d.). Academic boycott. BDS Movement. https://bdsmovement.net/academic-boycott

23 New Profile. (2025). Academia under orders: Militarism in Israeli academia — The collaboration between Israeli academia, the security establishment, and the military industry. [In Hebrew]. https://drive.google.com/file/d/14ZfAZn-ldt3hQSbtqegNoxE3uLHZoXlS/view

24 Kershner, I. (2024, December 5). Tel Aviv University developed dog-cameras for army unit linked to Gaza attacks. Middle East Eye. https://www.middleeasteye.net/news/tel-aviv-university-developed-dog-cameras-army-unit-linked-gaza-attacks

25 Al Jazeera. (2024, September 10). Israeli academia is directly complicit in the crimes of the state. Al Jazeera. https://www.aljazeera.com/opinions/2024/9/10/israeli-academia-is-directly-complicit-in-the-crimes-of-the-state

26 Kershner, I. (2024, December 5). Tel Aviv University developed dog-cameras for army unit linked to Gaza attacks. Middle East Eye. https://www.middleeasteye.net/news/tel-aviv-university-developed-dog-cameras-army-unit-linked-gaza-attacks

"I walk through the university knowing some of my fellow students are taking part in war rooms, designing more efficient methods to carry out the genocide in Gaza," said one who declined to be identified over fears they could be suspended for speaking out. "This marriage of militarism and educational institutions makes it extremely challenging to seriously engage with my studies, as I constantly question the ideology behind what we're being taught."

> This militarized knowledge regime is sustained by significant international backing. European funding. European (Horizon Europe: over €2.12 billion)[27] and U.S. institutions provide extensive funding, embedding them further within the military apparatus.[28] The high-tech sector, rooted in military intelligence is central to automated repression (e.g., NSO Group, IBM). According to several reports[29][30][31][32], Project Nimbus (Google & Amazon) and Azure Microsoft intensified support for combat operations. Employee protests (No Tech for Apartheid) against corporate complicity led to mass firings[33][34][35][36][37], underscoring the structural entanglement of corporate infrastructure with the occupation, enabling the shift from an "economy of occupation" to an "economy of genocide".[38]
>
> Ultimately, Israeli academia functions as a central R&D hub for the state's surveillance infrastructure. Universities such as the Technion and Tel Aviv University host specialized laboratories where AI-driven biometric systems and predictive policing algorithms are developed in direct coordination with the Israeli Ministry of Defense. This structural integration creates a seamless pipeline between academic innovation and military application, where Palestinians in the 1967 territories serve as the involuntary subjects for 'field-testing' these digital tools. Embedding cyber-surveillance within university missions turns academic production into an extension

27 Il Manifesto. (2025, May 31). Fondi europei per la ricerca, 1 miliardo alla difesa di Israele. il Manifesto. [In Italian]. https://ilmanifesto.it/fondi-europei-per-la-ricerca-1-miliardo-alla-difesa-di-israele

28 New Profile. (2025). Academia under orders: Militarism in Israeli academia — The collaboration between Israeli academia, the security establishment, and the military industry. [In Hebrew]. https://drive.google.com/file/d/14ZfAZn-ldt3hQSbtqegNoxE3uLHZoXlS/view

29 Albanese, F. (2025). From the economy of occupation to the economy of genocide: Report of the UN Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967. Office of the UN High Commissioner for Human Rights. https://www.un.org/unispal/document/

30 Davies, H. (2025, August 6). "A million calls an hour": Israel relying on Microsoft cloud for expansive surveillance of Palestinians. The Guardian. https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud

31 Davies, H., & Abraham, Y. (2025, January 23). Revealed: Microsoft deepened ties with Israeli military to provide tech support during Gaza war. The Guardian. https://www.theguardian.com/world/2025/jan/23/israeli-military-gaza-war-microsoft

32 Davies, H. (2025, October 29). Revealed: Israel demanded Google and Amazon use secret 'wink' to sidestep legal orders. The Guardian. https://www.theguardian.com/us-news/2025/oct/29/google-amazon-israel-contract-secret-code

33 Singh, K. (2025, August 29). Microsoft fires four workers on-site protests over company's ties to Israel. Reuters. https://www.reuters.com/sustainability/society-equity/microsoft-fires-four-workers-on-site-protests-over-companys-ties-israel-2025-08-29/

34 Singh, K. (2025, August 29). Microsoft fires four workers on-site protests over company's ties to Israel. Reuters. https://www.reuters.com/sustainability/society-equity/microsoft-fires-four-workers-on-site-protests-over-companys-ties-israel-2025-08-29/

35 De Vynck, G., & O'Donovan, C. (2024, April 16). Google workers arrested after protesting company's work with Israel. The Washington Post. https://www.washingtonpost.com/technology/2024/04/16/google-sit-in-employee-protest-nimbus-israel/

36 Middle East Eye. (2022, September 9). "Google chooses apartheid over justice": Workers protest Project Nimbus — Israel, Amazon and Google cloud deal. Middle East Eye. https://www.middleeasteye.net/news/project-nimbus-israel-apartheid-google-amazon-protests

37 Middle East Eye. (2024, April 18). War in Gaza: Google fires employees protesting contract with Israel's Project Nimbus. Middle East Eye. https://www.middleeasteye.net/news/war-gaza-google-fires-employees-protesting-contract-israel-project-nimbus

38 Albanese, F. (2025). From the economy of occupation to the economy of genocide: Report of the UN Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967. Office of the UN High Commissioner for Human Rights. https://www.un.org/unispal/document/

of remote-control occupation. While the physical destruction of Palestinian universities in Gaza (Scholasticide) constitutes a profound epistemic erasure requiring separate extensive study, it must be understood here as the violent counterpart to the rise of Israel's militarized digital hegemony.

Technological Control and Dependent Labor Regimes

Economic elimination is also achieved through territorial consolidation, using technology to expand settler control. The "Silicon Wadi" project in East Jerusalem is viewed by Palestinian residents as an instrument of Judaization—aiming to integrate the area into a settler vision (Al-Arnaout, 2021)[39][40]. Simultaneously, colonial economic relations structure Palestinian labor into dependent forms. Israeli regulations limit the Palestinian ICT sector's growth through import restrictions and spectrum denial. Outsourcing, framed as "coexistence," exploits Palestinian labor potential and low cost[41]. Employment models (e.g., NVIDIA) are contingent on Israeli permits and security approvals[42]. Inas, a senior engineer, describes waiting daily for a Shin Bet–issued permit to reach her workplace at a tech company in Herzliya, noting: "Sometimes I wait for hours—or cannot cross at all," and reflecting on the surreal image of passing the checkpoint with her laptop while her father crosses to build settlements. Such experiences exemplify what Clarno (Clarno, 2018a) terms **neoliberal apartheid**: a system that exploits Palestinian labor while sustaining dependency through administrative controls and coercive mobility regimes.

In response, some Palestinians pursue independent entrepreneurship to avoid subordination. Adnan founded his own start-up because he "did not want to be captive in an exploitative system," yet even his cross-border partnership faced obstruction, as Israeli authorities repeatedly detained him and his business partner, Palestinian from the 48' territories, at checkpoints—an effort he understood as designed to "keep dividing us constantly." Hazem similarly affirms that "any attempt at an independent Palestinian initiative…is halted by occupying forces," underscoring Israel's refusal to allow Palestinian technological autonomy. These dynamics reveal how economic elimination does not erase Palestinian economic activity but restructures it into dependent and reversible forms, with Israeli regulatory power determining access to markets, mobility, and growth. Since October 7, 2023, mobility restrictions deepened, and military destruction wiped out Gaza's ICT sector—formerly 30% of the oPt's IT economy [27]—erasing infrastructure and knowledge.

4.1.3 Epistemic Elimination: Digital Platforms and Corporate Workplaces

Digital platforms are critical arenas for epistemic elimination, the systematic destruction of the ability to produce and circulate knowledge. In digital settler colonialism, this manifests as algorithmic epistemic violence that determines whose speech is amplified and whose is erased.

39 See more of the project here: https://www.jerusalem5800.com/about/the-project

40 See more of the project here: https://sustainabledevelopment.un.org

41 Alliance for Middle East Peace. (2025, November 20). Working together: Israeli and Palestinian coexistence in tech. https://www.allmep.org/allmep-resources/working-together-israeli-and-palestinian-coexistence-in-tech/

42 The Times of Israel. (2020, October 15). US firm Nvidia to employ 100 West Bank engineers as salaried workers. https://www.timesofisrael.com/us-firm-nvidia-to-employ-100-west-bank-engineers-as-salaried-workers/

7amleh (2024)[43] documents systematic suppression of Palestinian content through biased moderation, creating epistemic asymmetry: Palestinians are hyper-visible to surveillance but inaudible in public discourse. Post-October 7, this intensified. Meta's platforms amplified violence and dehumanization in Hebrew (e.g., "human animals"), allowing incitement to circulate while systematically censoring Palestinian narratives.[44][45] The Israeli army itself operated a Telegram channel publishing graphic content and dehumanizing language, confirming incitement originated from the IDF.[46] This disparity reveals a double standard embedded in Meta's policies where tolerance for Hebrew incitement amounts to complicity. [47]

Epistemic elimination extends into the "neutral" spaces of high-tech workplaces. Digital repression is mirrored in tech hubs where Palestinian engineers are silenced or dismissed.[48][49] A survey by NAS[50] documents widespread fear among Palestinian engineers in Israel—44% afraid to attend work - highlighting how the workplace reinforces societal suspicion and fails to uphold diversity during crisis. [51] This creates an epistemic hostile environment, where the Palestinian professional must choose between their career and their reality.

Furthermore, the discourse over diversity itself has been silenced. While Israeli tech international companies often market themselves globally through the lens of "coexistence" and "inclusion," the post-October 7 reality has exposed these frameworks as superficial. Diversity is tolerated only as long as it remains "politically mute." This misinterpretation is mirrored in the American and Israeli "Progressive" tech circles, which have adopted the stance known as "Progressive Except for Palestine" (PEP) offered by Ghassan Al-Hajj (Al-Hajj, 2019).

In this configuration, the high-tech workplace functions as a secondary border, where the "ideal" Palestinian worker is politically neutralized and rendered invisible.

43 7amleh – The Arab Center for the Advancement of Social Media. (2024, August 28). 70% of Palestinian youth in Israel practice self-censorship online. https://7amleh.org/post/palestinian-youth-practice-self-censorship-online-en

44 7amleh – The Arab Center for the Advancement of Social Media. (2024, August 28). 70% of Palestinian youth in Israel practice self-censorship online. https://7amleh.org/post/palestinian-youth-practice-self-censorship-online-en

45 7amleh – The Arab Center for the Advancement of Social Media. (2025, September 2). Meta's role in amplifying harmful content during genocide in Gaza. https://7amleh.org/post/meta-s-role-during-genocide-en

46 7amleh – The Arab Center for the Advancement of Social Media. (2025, September 2). Meta's role in amplifying harmful content during genocide in Gaza. https://7amleh.org/post/meta-s-role-during-genocide-en

47 7amleh – The Arab Center for the Advancement of Social Media. (2025, September 2). Meta's role in amplifying harmful content during genocide in Gaza. https://7amleh.org/post/meta-s-role-during-genocide-en

48 7amleh – The Arab Center for the Advancement of Social Media. (2025, September 2). Meta's role in amplifying harmful content during genocide in Gaza. https://7amleh.org/post/meta-s-role-during-genocide-en

49 7amleh – The Arab Center for the Advancement of Social Media. (2024). Delete the Issue: Tech Worker Testimonies on Palestinian Advocacy and Workplace Suppression [PDF report]. https://7amleh.org/storage/Advocacy%20Reports/Delete%20the%20issue-11.11.pdf

50 NAS Research & Consulting. (2024, January). Arabs in Hi-Tech: From Diversity to Inclusion [PDF report]. https://www.nasconsulting.co.il/wp-content/uploads/2024/01/NAS_Arabs-in-Hi-Tech-Diversity-to-Inclusion_En_Tsofen_Aug23.pdf

51 Gams, N. (2024, January 22). "It's hard to say what would be different if I were Israeli, but I come from a country ..." TheMarker. [In Hebrew]. https://www.themarker.com/career/2024-01-22/ty-article-magazine/.premium/0000018d-2bf2-daf5-a1bf-aff282150000

4.2 RESISTING ELIMINATION: DIGITAL SUMŪD AS A MULTI-LAYERED ARCHITECTURE OF PRESENCE, SURVIVAL AND FUTURITY

Digital sumūd materializes through counter-infrastructures, archives, and alternative networks that resist physical, economic, and epistemic elimination. Bombardment, siege, displacement, starvation, infrastructural collapse, corporate entanglement, censorship, and scholasticide are not discrete processes but mutually reinforcing mechanisms designed to produce disappearance. In response, digital sumūd emerges as a layered architecture of resistance that sustains Palestinian life, visibility, and futurity across these domains. Rather than constituting isolated online acts, digital sumūd materializes through four interrelate practices: Material and infrastructural persistence, Connectivity as an act of Care and Survival, Digital Witnessing, Counter-Archives, and Institutional Mobilization, Rebuilding the nation as an act of digital Sumūd and Futurity

4.2.1 Connectivity and Infrastructural Persistence

The empirical evidence shows Palestinians respond to physical elimination—bombardment, displacement, siege, and engineered communication blackouts—by constructing improvised infrastructures that sustain life, connection, and visibility. Diaspora volunteers, digital-rights organizations, and civilians mobilized eSIMs, VPNs, mesh networks, satellite links, and mirrored accounts to counter deliberate disconnection. Rather than treating connectivity as a secondary communicative tool, the findings demonstrate that digital infrastructure becomes a survival architecture. Staying online is not symbolic—it is existential. Campaigns such as #ConnectingGaza[52] and Reconnect Gaza[53] frame connectivity not only as a communicative right but as a matter of survival, aligning with decolonial design scholarship in which infrastructural practice becomes a means of repurposing technology for liberation.

During communication blackouts, maintaining digital connectivity becomes a life-affirming act. Grassroots engineers and NGOs—such as the Association for Progressive Communications (APC) and Access Now's KeepItOn Coalition—have also supported mesh networks, satellite communication, and offline archiving systems to preserve the flow of information. These acts of technological care expand the meaning of sumūd beyond defiance to include relational maintenance and mutual aid. Here, digital sumūd signifies the ethical practice of "staying online" as a collective refusal of erasure.

Individual narratives deepen this picture by showing how digital survival is inseparable from physical survival. Yasmina, a Palestinian tech worker in Gaza later killed in the 2024 airstrikes, described how electricity and internet shortages repeatedly disrupted her work. Under bombardment, she improvised continuity:

52 Landy, H., & Shabana, Y. (2025, October –). Tens of thousands of Palestinians in Gaza are staying connected to the world via donated eSIMs. Quartz. https://qz.com/tens-of-thousands-of-palestinians-in-gaza-are-staying-c-1851078107

53 7amleh – The Arab Center for the Advancement of Social Media. (2025, February 26). #ReconnectGaza – Reconnecting Gaza, empowering the future. https://7amleh.org/reconnectgaza/en/

"There was barely any electricity... My father helped by charging the laptop at the mosque, which always had a generator... He did this five times a day, during each of the five prayers."

Her account reveals digital survival as a collective family effort rooted in care and endurance. The mosque's generator—intended for worship—became part of an improvised network where religious space, family labor, and technological necessity converged. Connectivity emerged not from formal infrastructure but from relational coordination and sacrifice. In this context, remaining online was more than a technical task; it was an act of survival and visibility. Yasmina's continued presence depended on intergenerational care and the deliberate maintenance of connection. Digital sumūd thus materialized through everyday practices of endurance.

The connectivity extends beyond the household to transnational networks. Amid acute food insecurity in Gaza[54]—documented by the Food and Agriculture Organization (FAO)[55] and the World Food Programme (WFP)[56]-digital platforms became channels for survival and, grassroots solidarities have emerged. Jordanian chef Yasmin Nasir, for example, used Instagram to share ways of preparing meals from scarce ingredients.[57] Her activism illustrates how digital platforms facilitate cross-border relational solidarities, consistent with scholarship on affective forms of digital engagement.

Such exchanges demonstrate how connectivity operates as distributed care across borders. Through affective and practical solidarities, digital platforms become infrastructures of mutual aid. Connectivity enables emotional reassurance, informational exchange, and material survival strategies to move across territorial constraints.

Digital **sumūd** therefore expands beyond defiance to encompass connectivity as a deliberate practice of care and survival. To "stay online" is to refuse social death, to insist on relational continuity even when physical infrastructures are destroyed. Connectivity becomes both lifeline and political act—an everyday enactment of presence against disappearance.

4.2.2 Digital Witnessing, Counter-Archives, and Institutional Mobilization

This theme traces how Palestinians mobilize digital tools as a multidimensional strategy against physical and epistemic elimination. Through real-time witnessing, counter-archiving, and institutional advocacy, digital space becomes not only a terrain of surveillance but also a site of sumūd (steadfastness), narrative authority, and historical continuity.

54 World Health Organization. (2025, August 22). Famine confirmed for first time in Gaza. https://www.who.int/news/item/22-08-2025-famine-confirmed-for-first-time-in-gaza?utm_source

55 The Food and Agriculture Organization

56 The World Food Programme

57 See Yasmin's Instagram page: https://www.instagram.com/yasmin.nasir

Digital witnessing as Resistance.

Digital witnessing and documentation by journalists such as Motaz Azaiza[58] and Bisan Owda[59] (Image 1 and 2) demonstrate how visibility becomes a form of resistance. Reporting from Gaza amid extreme danger, they livestream, photograph, and archive events in real time, countering both restrictions on foreign media and platform moderation practices. Here, documentation becomes a political act: it challenges narrative monopolies and produces an alternative evidentiary record. Visibility itself becomes an act of electronic resistance (Khoury-Machool, 2007; Shehadeh, 2023).



Image 1



Image 2

Digital Solidarity and Survival.

Beyond bombardment, starvation constitutes another dimension of elimination. Agencies such The Food and Agriculture Organization (FAO)[60] and the World Food Programme (WFP)[61] report unprecedented levels of acute food insecurity in Gaza.[62] In response, transnational solidarities emerge online. Jordanian chef Yasmin Nasir used Instagram to share improvised cooking methods, offering practical knowledge and symbolic support. [63] Social media thus operates not only as a channel of information but as a space of relational care, sustaining life through shared knowledge.

Counter-Archives and Epistemic Disobedience.

In the face of censorship and destruction Palestinians increasingly turned to digital preservation (Ghaddar, 2025). As one scholar notes, "this systematic erasure is not new".[64] Consequently, Initiatives such as the Palestinian Museum Digital Archive and Decolonize Palestine assert Palestinian perspectives as authoritative, refusing colonial control over what counts as

58 Motaz Azaiza—a journalist and photographer with a degree in English Translation from Al-Azhar University, one of several universities destroyed in recent Israeli airstrikes—emerged as one of the most influential visual chroniclers of the war. Beginning his career as a freelance photographer, Azaiza became one of the most widely followed and trusted voices reporting from Gaza during the Israeli military assault that began on October 7. Time selected one of his photos, depicting a child under the rubble caused by an Israeli bombing, as one of the ten most representative images of 2024 (See the link: https://www.arabnews.com/node/2612324/amp?utm_source)

59 Bisan - a digital content creator and youth activist from Gaza with a degree in Business Economics, has become internationally recognized for her on-the-ground reporting. Through her social-media series "This is Bisan from Gaza" and "I'm Still Alive," she documents daily life under bombardment with a blend of immediacy and narrative clarity that has reached millions. Her work earned global acclaim, winning an Emmy Award after being nominated in the category of Outstanding Hard News Feature Story: Short Form at the 2024 News and Documentary Emmy Awards.

60 The Food and Agriculture Organization

61 The World Food Programme

62 World Health Organization. (2025, August 22). Famine confirmed for first time in Gaza. https://www.who.int/news/item/22-08-2025-famine-confirmed-for-first-time-in-gaza?utm_source

63 See Yasmin's Instagram page: https://www.instagram.com/yasmin.nasir

64 Wilson, L. (2025, June 27). Historicide in Gaza: Israel's destruction of official and personal archives is changing how Palestine's story can be told. New Lines Magazine. https://newlinesmag.com/essays/historicide-in-gaza/

legitimate knowledge. Micro-archives—recording, screenshotting, and sharing—circulate widely during blackouts, while projects like Fighting Erasure coordinate transnational preservation efforts. Together, these practices form an infrastructure of memory and epistemic disobedience that safeguards historical continuity and contests epistemic hierarchies (Mignolo, 2009, 2011).

Institutional and Corporate Accountability.

Digital sumūd also operates through organized civil society advocacy. Organizations such as 7amleh, Adalah, Sada Social Center, and SMEX document algorithmic bias and content removal, transforming individual cases into evidence of structural censorship. Advocacy by Facebook, We Need to Talk[65] prompted an independent audit by Business for Social Responsibility, which confirmed systemic moderation disparities. [66]

Parallel mobilization extends into academia and the tech sector. The Boycott, Divestment and Sanctions movement and Palestinian Campaign for the Academic and Cultural Boycott of Israel challenge university and corporate ties to Israeli military and surveillance infrastructures.[67] PACBI[68] argues that the boycott disrupts knowledge pipelines that sustain military and surveillance regimes.[69] The intensification of global student activism post-October 7 exposed the "hypocrisy" of prestigious universities, leading BDS co-founder Omar Barghouti to frame the movement as "Palestine's South Africa moment".[70] This momentum has led dozens of universities to adopt divestment or suspend partnerships, marking unprecedented global academic engagement.



Image 3



Image 4

Within global tech firms, coalitions such as No Tech for Apartheid oppose projects like Project Nimbus. [71] (See Image 3), a cloud-computing contract

65 **7amleh – The Arab Center for the Advancement of Social Media. (n.d.).** Delete the issue (Issue 11.11). https://www.7amleh.org/storage/Advocacy%20Reports/Delete%20the%20issue-11.11.pdf

66 Human Rights Watch. (2022, September 27). Statement Regarding BSR's HRA for Meta on Palestine & Israel. https://www.hrw.org/news/2022/09/27/statement-regarding-bsrs-hra-meta-palestine-israel

67 BDS Movement. (n.d.). Academic Boycott. https://bdsmovement.net/academic-boycott

68 The Palestinian Campaign for the Academic and Cultural Boycott of Israel

69 BDS Movement. (n.d.). Academic Boycott. https://bdsmovement.net/academic-boycott

70 The Guardian. (2024, June 4). BDS founder hails campus protests for taking Israeli divestment mainstream. https://www.theguardian.com/us-news/article/2024/jun/04/bds-omar-barghouti-israel-campus-protests

71 Middle East Eye. (2022, September 2). Project Nimbus: Google employee accuses tech giant of profiteering from Palestinian pain. Middle East Eye. https://www.middleeasteye.net/news/palestine-google-project-nimbus-employee-accuses-profiteering-pain

between Google, Amazon, and the Israeli government. [72] Direct-action campaigns such as Shut Elbit Down[73] (See image 4), target firms implicated in surveillance technologies, predictive analytics, and cloud infrastructure.

Collectively, these initiatives function as an economic and epistemic resistance toolkit, exposing corporate complicity and contesting digital colonial power from within its own infrastructures

4.2.3 Rebuilding the nation as an act of digital Sumūd and Futurity

This theme conceptualizes nation-building under conditions of siege not only as a post-colonial aspiration, but as an ongoing practice of **sumūd** (steadfastness) oriented toward futurity and building the economic nation. Palestinian technological and entrepreneurial initiatives demonstrate that rebuilding is not limited to physical reconstruction; it also entails the creation of alternative economic, epistemic, and infrastructural tech ecosystems virtually and physically. In this sense, technological practice becomes both a survival strategy and a prefigurative political act — an effort to materialize autonomy within structures of constraint.

Constructing Alternative Ecosystems Palestinian tech initiatives serve as institutional counterweights to structural dependency. Gaza Sky Geeks (digital incubator) and MENA Alliances (founded by Abeer Abu Ghaith - See image 6 below) connect workers to global markets, circumventing mobility restrictions and reducing reliance on Israeli labor. Palestine Open Maps reconstructs erased geographies, while BuildPalestine strengthens community-based innovation. These initiatives build sustainable, autonomous economic ecosystems (Althalathini et al., 2020; Althalathini & Tlaiss, 2023; Aouragh, 2011; Rindova et al., 2009), embodying entrepreneurial agency and decolonial technological practice despite the settler colonial reality.



Image 6

Abeer, a tech entrepreneur from Jenin, articulated this logic succinctly. Despite movement restrictions and the absence of an airport, she emphasized the portability and autonomy enabled by digital labor:

"The laptop is very important; I always told my parents and my sister who work that the most important thing is the laptop. Even if all the roads were closed in your face, [the laptop] is still your portal/ door to the world...It was the only thing I needed to connect with people and recruit people from Gaza to work with me"

Abeer's testimony highlights how digital labor transforms spatial restriction into networked mobility. The laptop operates as a micro-infrastructure of autonomy, enabling participation in global markets despite territorial enclosure and movement constraints. Connectivity thus functions not only as an economic strategy but as a political practice that challenges-imposed immobilization. By recruiting workers from Gaza, Abeer also

72 The Guardian. (2025, August 19). Microsoft workers protest Washington-Israel tech deal. https://www.theguardian.com/technology/2025/aug/19/microsoft-workers-protest-washington-israel

73 The Guardian. (2025, August 19). Microsoft workers protest Washington-Israel tech deal. https://www.theguardian.com/technology/2025/aug/19/microsoft-workers-protest-washington-israel

demonstrates how digital platforms re-link fragmented Palestinian geographies, fostering internal economic cohesion. In line with scholarship on entrepreneurial agency and digital transnationalism (Aouragh, 2011; Rindova et al., 2009), such initiatives position technology as an infrastructure of **sumūd** — a means of actively reorganizing economic relations under conditions of constraint rather than merely enduring them.



Image 7

Majd, another tech entrepreneur from Gaza, exemplifies a materially grounded form of digital **sumūd**. Drawing on her technical expertise, she founded SunBox, a solar-energy startup that provided sustainable electricity and water access to tens of thousands of residents, including vulnerable communities without the need of Israel. "We barely have electricity, before October 7th we had only 6 hours of electricity. This is where the idea of Sunbox came from". In the context of infrastructural collapse and chronic energy shortages, renewable technology functioned simultaneously as a survival mechanism and as a model for decentralized autonomy.

After an airstrike destroyed her home, Majd and her father developed GreenCake, an initiative that transformed rubble from demolished buildings into recycled construction materials. This project earned her the nickname "Bint al-Hajar" (The Brick Lady). (See image 7). Her trajectory illustrates how technological skill can be mobilized to reconstruct both material conditions and social infrastructure under extreme precarity. She shared:

"My friends were murdered during one of the military invasions.... This incident had a huge impact; our house was also destroyed. I developed a sense of frustration, like how long are we going to wait for Qatar and the United Nations to build our town, and how long are we going to wait for the help of international organizations when ninety-four percent of us are educated? so why don't we produce? I have always had this curiosity, you see people abroad producing, so why can't we produce as well?"



Image 8

The war on Gaza, however, severely disrupted these projects. SunBox was buried under rubble. On her Facebook page, Majd wrote (See image 8):

"All the memories, certificates, awards, gifts, and photos—my entire life's work—have disappeared and been erased under the rubble."

This statement reflects not only material destruction but epistemic loss — the erasure of professional trajectories and accumulated recognition.

Similarly, Dalia, another tech entrepreneur from Gaza, posted an image of the damaged premises of Gaza Sky Geeks shown on the following page (See image 9). Beneath the photograph of the ruins, she wrote:

"The Gaza I knew has been completely transformed by the destruction caused by the occupation's attacks. I believe with all my heart that we will rebuild it like a phoenix rising from the ashes—full of life!".

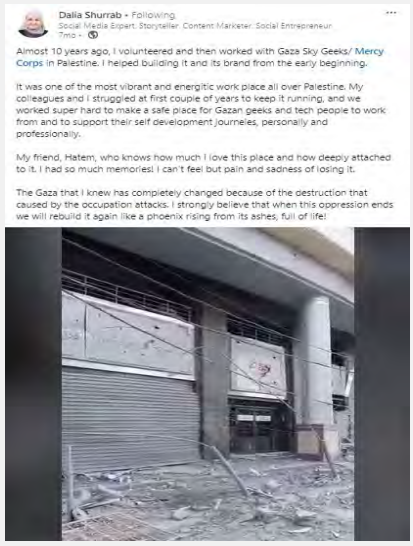


Image 9

These testimonies reveal how digital platforms mediate destruction and futurity simultaneously. Social media platforms become a space where loss is documented, grief is articulated, and reconstruction is imagined. Individual resilience is transformed into communicative resistance: an assertion of presence, continuity, and collective determination. Such cases resonate with scholarship suggesting that technological entrepreneurship can operate as an emancipatory pathway for marginalized communities seeking autonomy and collective transformation (Awwad & Toyama, 2024; Mignolo, 2009; Rindova et al., 2009; Shehadeh, 2023). Tech innovation, in this framing, is not detached from politics; it is embedded within struggles over survival, dignity, and future-making.

At the end, rebuilding through technology and digital platforms is not postponed to a hypothetical post-war future. It unfolds amid destruction as an act of **sumūd** and as a claim to futurity. Through alternative digital ecosystems, renewable energy initiatives, entrepreneurial reconstruction, and online testimony, Palestinians enact a form of nation-building grounded in technological skill and collective imagination. These practices demonstrate that technology can serve not only as an instrument of control but also as a medium for survival, reconstruction, and political agency. The rebuilding of Gaza thus emerges as both a material and epistemic project — one that insists on life, continuity, and the right to imagine a better future.

5. CONCLUSION

This study shows that the Israeli occupation has entered a fully digital phase in which algorithmic systems, data infrastructures, and innovation economies now perform functions once carried out by soldiers and bureaucrats. Remote-control governance—through AI-assisted targeting, biometric surveillance, automated checkpoints, and network control—intensifies rather than replaces colonial domination. Palestinians become hyper-visible as data subjects yet illegible as political actors, rendered knowable to machines while erased within humanitarian, academic, and innovation discourses. This is the automation of apartheid: the translation of racialized governance into computational form. The analysis identifies three interlocking modes of digital elimination: physical (automated targeting and systems like Blue Wolf/Lavender), economic (embedding occupation in global markets and

denying technological sovereignty via the civil–military–academic nexus), and epistemic (platform censorship, archival destruction, and scholasticide).

Against this regime, Palestinians cultivate digital sumūd—a form of epistemic disobedience that builds alternative communication, archiving, and community infrastructures. Through distributed documentation and transnational solidarity, they reclaim digital space for resistance and endurance.

Resisting algorithmic occupation requires dismantling oppressive digital systems and designing decolonial technological futures that prioritize Palestinian digital sovereignty, moving beyond narrow Western AI-ethics frameworks. The rise of digital sumūd underscores that struggles over data and AI are integral to liberation and accountability.

REFERENCES

- 7amleh. (2024). Delete the issue-11.11 Tech Worker Testimonies on Palestinian Advocacy & Workplace suppression. https://7amleh.org/storage/Advocacy%20Reports/Delete%20the%20issue-11.11.pdf
- Abu-Lughod, L. (2020). Imagining Palestine's Alter-Natives: Settler Colonialism and Museum Politics. Critical Inquiry, (47), 1–27.
- Ahmad, R. S. (2021). The Expansion of Digital Surveillance in Jerusalem and Impact on Palestinians Rights. In 7amleh –The Arab Center for Social Media Advancement The.
- Al-Arnaout, A. al-R. (2021). A " Silicon " Disaster Threatening Wadi al-Jawz. Jerusalem Quarterly, (85), 125–131. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.palestine-studies.org/sites/default/files/jq-articles/A%20%E2%80%9C-Silicon%E2%80%9D%20Disaster%20Threatening%20Wadi%20al-Joz.pdf
- Albanese, F. (2025). From economy of occupation to economy of genocide (A/HRC/59/23). https://www.un.org/unispal/document/a-hrc-59-23-from-economy-of-occupation-to-economy-of-genocide-report-special-rapporteur-francesca-albanese-palestine-2025/
- Al-Hajj, G. (2019). Palestine and the West: Colonialism and the Lack of Belonging. Majallat al-Dirasat al-Filastiniyya, Institute for Palestine Studies, Summer 2019(119). https://www.palestine-studies.org/en/node/235542
- Al-Salhi, A. (2021). The Palestinian Public's Perception of Palestinian CSOs. In 7amleh - The Arab Center for the Advancement of Social Media (Number October).
- Althalathini, D., Al-Dajani, H., & Apostolopoulos, N. (2020). Navigating Gaza's Conflict through Women's Entrepreneurship. Journal of Small Business Management, 58(4), 678–695.
- Althalathini, D., & Tlaiss, H. A. (2023). Of resistance to patriarchy and occupation through a virtual bazaar: an institutional theory critique of the emancipatory potential of Palestinian women's digital entrepreneurship. Entrepreneurship and Regional Development. https://doi.org/10.1080/08985626.2023.2241412
- Amit, G. (2011). Salvage or Plunder? Israel's "Collection" of Private Palestinian Libraries in West Jerusalem. Journal of Palestine Studies, 40(4), 6–23. https://www.palestine-studies.org/en/node/42473
- Aouragh, M. (2011). Palestine online: Transnationalism, the Internet and the construction of identity. In Palestine Online. I.B.Tauris. https://doi.org/10.5040/9780755607884
- Avis, M., Marciniak, D., & Sapignoli, M. (2025). States of Surveillance: Ethnographies of New Technologies in Policing and Justice. Routledge. https://www.routledge.com/Routledge-
- Awwad, G., & Toyama, K. (2024). Digital Repression in Palestine. Conference on Human Factors in Computing Systems - Proceedings, 15. https://doi.org/10.1145/3613904.3642422;WGROUP:STRING:ACM
- Bauman, Z. (1989). Modernity and the Holocaust. Cornell University Press.
- Bevilacqua, I. (2022). E-scaping apartheid: Digital ventures of Zionist settler colonialism. Human Geography(United Kingdom), 15(2), 220–228. https://doi.org/10.1177/19427786211055780
- Busse, J. (2022). Everyday life in the face of conflict: Sumud as a spatial quotidian practice in Palestine. Journal of International Relations and Development, 25(3), 583. https://doi.org/10.1057/S41268-022-00255-1
- Clarno, A. (2018a). Neoliberal Apartheid: Palestine/Israel and South Africa after 1994. In The University of Chicago Press. The University of Chicago Press. https://doi.org/10.1177/0094306118779814e

- Clarno, A. (2018b). Neoliberal colonization in the West Bank. Social Problems, 65(3), 323–341. https://doi.org/10.1093/socpro/spw055
- Couldry, N., & Mejias, U. A. (2019). The costs of connection: How data is colonizing human life and appropriating it for capitalism. Stanford University Press.
- Fanon, F. (1963). The wretched of the earth. Grove Press.
- Foucault, M. (2008). The Birth of Biopolitics: Lectures at the Collège De France 1978-1979 (G. Burchell, Tran.). Palgrave Macmillan. https://doi.org/10.22439/fs.v0i7.2640
- Getzoff, J. F. (2020). Start-up nationalism: The rationalities of neoliberal Zionism. Environment and Planning D: Society and Space, 38(5), 811–828. https://doi.org/10.1177/0263775820911949
- Ghaddar, J. J. (2025). Palestine as provenance: archiving against genocide from Gaza to South Lebanon (Jabal Amil). Archival Science 2025 25:3, 25(3), 20-. https://doi.org/10.1007/S10502-025-09484-Y
- Gillespie, T. (2018). Custodians of the Internet: platforms, content moderation, and the hidden decisions that shape social media. Yale University Press.
- Giroux, H. A. (2025). Scholasticide: Waging War on Education from Gaza to the West. Https://Doi.Org/10.3366/Hlps.2025.0348, 24(1), 1–16. https://doi.org/10.3366/HLPS.2025.0348
- Hammami, R. (2005). On the Importance of Thugs The Moral Economy of a Checkpoint. Jerusalem Quarterly., (22/23), 22–28.
- Johnson, D. (2019). Occupation: Neoliberalism' s Role in Palestinian Apartheid. In Locus: The Seton Hall Journal of Undergraduate Research (Vol. 2).
- Jorisch, Avi. (2018). Thou shalt innovate : how Israeli ingenuity repairs the world. Gefen Publishing House Ltd. https://books.google.com/books/about/Thou_Shalt_Innovate.html?id=k_uEswEACAAJ
- Khoury-Machool, M. (2007). Palestinian Youth and Political Activism: The Emerging Internet Culture and New Modes of Resistance. Policy Futures in Education, 5(1), 17–36. https://doi.org/10.2304/PFIE.2007.5.1.17
- Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. Race and Class, 60(4), 3–26. https://doi.org/10.1177/0306396818823172
- Kwet, M. (2022). Digital Colonialism and Infrastructure-as-Debt. University of Bayreuth African Studies Online, 65–77. https://orcid.org/0000-0002-3304-5649.
- Last, D. M. (2007). Economic Peace-Building to Support Israeli-Palestinian Disengagement. In Royal Military College of Canada (Number May).
- Lentin, R. (2020). Palestinian Lives Matter: Racialising Israeli Settler-Colonialism. Journal of Holy Land and Palestine Studies, 19(2), 133–149. https://doi.org/10.3366/HLPS.2020.0238
- Lloyd, D., & Wolfe, P. (2016). Settler colonial logics and the neoliberal regime. Settler Colonial Studies, 6(2), 109–118. https://doi.org/10.1080/2201473X.2015.1035361
- Loewenstein, A. (2023). The Palestine Laboratory: How Israel Export the technology of occupation around the world. Verso Books. https://www.researchgate.net/publication/377691958
- Maggor, E. (2020). The Politics of Innovation Policy: Building Israel's "Neo-developmental" State. Politics and Society. https://doi.org/10.1177/0032329220945527
- Masalha, N. (2012). Appropriating History: Looting of Palestinian Records, Archives and Library Collections, 1948-2011. In The Palestine Nakba Decolonising History, Narrating the Subaltern, Reclaiming Memory (pp. 135–147). Zed Books.
- Mignolo, W. (2009). Epistemic Disobedience, Independent Thought and Decolonial Freedom. Theory, Culture & Society, 26(8), 159–181. https://doi.org/10.1177/0263276409349275;WEBSITE:WEBSITE:SAGE;-JOURNAL:JOURNAL:TCSA;WGROUP:STRING:PUBLICATION

- Mignolo, W. (2011). Epistemic Disobedience and the Decolonial Option: A Manifesto. TRANSMODERNITY: Journal of Peripheral Cultural Production of the Luso-Hispanic World, 1(2). https://doi.org/10.5070/t412011807
- Mignolo, W., & Walsh, C. (2018). On Decoloniality: Concepts, Analytics, Praxis. Duke University Press. https://books.google.com/books/about/On_Decoloniality.html?hl=it&id=l8hcDwAAQBAJ
- Milan, S., & Treré, E. (2019). Big Data from the South(s): Beyond Data Universalism. Television and New Media, 20(4), 319–335. https://doi.org/10.1177/1527476419837739;-JOURNAL:JOURNAL:TVNA;PAGE:STRING:ARTICLE/CHAPTER
- Musleh, A. H. (2018). Designing in Real-Time: An Introduction to Weapons Design in the Settler-Colonial Present of Palestine. Design and Culture, 10(1), 33–54. https://doi.org/10.1080/17547075.2018.1430992
- Noble, S. U. (2018). Algorithms of Oppression How Search Engines Reinforce Racism. NYU Press. https://www.degruyterbrill.com/document/doi/10.18574/nyu/9781479833641.001.0001/html
- Peeters, R., & Schuilenburg, M. (2023). Algorithmic Governance: Technology, Knowledge and Power. In The SAGE Handbook of Digital Society (pp. 439–457). SAGE Publications Ltd. https://doi.org/10.4135/9781529783193.n25
- Peled-Elhanan, N. (2012). Palestine in Israeli School Books Ideology and Propaganda in Education. I.B. Tauris.
- Rijke, A., & Van Teeffelen, T. (2014). To Exist Is To Resist: Sumud, Heroism, and the Everyday | Institute for Palestine Studies. Jerusalem Quarterly , (59). https://www.palestine-studies.org/en/node/165375
- Rindova, V., Barry, D., & Ketchen, D. J. (2009). Entrepreneuring as Emancipation. In Academy of Management Review (Vol. 34, Number 3, pp. 477–491). Academy of Management. https://doi.org/10.5465/amr.2009.40632647
- Sabbagh-Khoury, A. (2022). Tracing Settler Colonialism: A Genealogy of a Paradigm in the Sociology of Knowledge Production in Israel. Politics and Society, 50(1), 44–83. https://doi.org/10.1177/0032329221999906
- Sabbah-Karkabi, M., & Abu-Rabia-Queder, S. (2025). The politics of silence: Palestinian faculty and the struggle for voice in Israeli academia in times of war*. Ethnic and Racial Studies, 1–19. https://doi.org/10.1080/01419870.2025.2561759;JOURNAL:JOURNAL:RERS20;REQUESTEDJOURNAL:JOURNAL:RERS20;WGROUP:STRING:PUBLICATION
- Sa'di, A. H. (2021). Israel's settler-colonialism as a global security paradigm. Race and Class, 63(2), 21–37. https://doi.org/10.1177/0306396821996231
- Sela, R. (2018). The Genealogy of Colonial Plunder and Erasure– Israel's Control over Palestinian Archives. Social Semiotics, 28(2), 201–229. https://doi.org/10.1080/10350330.2017.1291140
- Senor, Dan., & Singer, Saul. (2009). Start-up nation : the story of Israel's economic miracle. In Twelve. Twelve.
- Shalhoub-Kevorkian, N. (2015). Security theology, surveillance and the politics of fear. In Security Theology, Surveillance and the Politics of Fear. Cambridge University Press. https://doi.org/10.1017/CBO9781316159927
- Shalhoub-Kevorkian, N. (2017). Settler colonialism, surveillance, and fear. In Israel and its Palestinian Citizens: Ethnic Privileges in the Jewish State. https://doi.org/10.1017/CBO9781107045316.012
- Shehadeh, H. (2023). Palestine in the Cloud: The Construction of a Digital Floating Homeland. Humanities (Switzerland), 12(4). https://doi.org/10.3390/h12040075

- Shihadeh, M. (2024). The War on Gaza and Israel's Technology Sector. https://arabcenterdc.org/resource/the-war-on-gaza-and-israels-technology-sector/
- Siegel M., S. (2015). Let There Be Water: Israel's Solution for a Water-Starved World. Macmillan.
- Swed, O., & Butler, J. S. (2015). Military capital in the Israeli Hi-tech industry. Armed Forces and Society, 41(1), 123–141. https://doi.org/10.1177/0095327X13499562
- Tariq, D. (2024). Gaza's Genocide and Israel's Military-Industrial Complex. https://www.palestine-studies.org/en/node/1655307?utm_source=chatgpt.com
- Tarvainen, A., & Challand, B. (2024). Innovation as erasure: Palestine and the new regional alliances of technology. Transactions of the Institute of British Geographers, 49(2). https://doi.org/10.1111/tran.12663
- Tatour, L. (2019). Citizenship as Domination: Settler Colonialism and the Making of Palestinian Citizenship in Israel. The Arab Studies Journal, 2(27), 839. https://ssrn.com/abstract=3533490
- Tawil-Souri, H. (2012). Digital Occupation: Gaza's High-Tech Enclosure. Journal of Palestine Studies, 41(2), 27–43. https://www.jstor.org/stable/10.1525/jps.2012.xli.2.27%0AJSTOR
- Tawil-Souri, H., & Aouragh, M. (2014). INTIFADA 3 . 0 ? CYBER COLONIALISM AND PALESTINIAN RESISTANCE. The Arab Studies Journal, 22(1), 102–133.
- Veracini, L. (2011). Introducing: settler colonial studies. Settler Colonial Studies, 1(1), 1–12. https://doi.org/10.1080/2201473X.2011.10648799
- Veracini, L. (2015). The Settler Colonial Present. Springer. https://books.google.it/books?hl=it&lr=&id=1U9OCgAAQBAJ&oi=fnd&pg=PP1&dq=Veracini,+L.+(2015).+The+settler+colonial+present.+Springer.&ots=BHiCY7DQm-J&sig=vLPGe1JJd4qXe_dj_rYKqhZK68s#v=onepage&q=Veracini%2C%20L.%20(2015).%20The%20settler%20colonial%20present.%20Springer.&f=false
- Wildeman, J. (2019). Neoliberalism as Aid for the Settler Colonization of the Occupied Palestinian Territories After Oslo. In Palestine and Rule of Power (pp. 153–174). Springer International Publishing. https://doi.org/10.1007/978-3-030-05949-1_7
- Wind, Maya. (2024). Towers of ivory and steel : how Israeli universities deny Palestinian freedom. 278.
- Wolfe, P. (2006). Settler colonialism and the elimination of the native. Journal of Genocide Research, 8(4), 387–409. https://doi.org/10.1080/14623520601056240
- York, J. C. (2012). PALESTINE ONLINE: TRANSNATIONALISM, THE INTERNET AND THE CONSTRUCTION OF IDENTITY by Miriyam Aouragh. The Arab Studies Journal, 20(1), 214–217. https://www.jstor.org/stable/23265851?seq=1#metadata_info_tab_contents
- Zureik, E. (2001). Constructing Palestine through surveillance practices. British Journal of Middle Eastern Studies, 28(2), 205–227. https://doi.org/10.1080/13530190120083086
- Zureik, E. (2016a). Israel's colonial project in Palestine: Brutal pursuit. Routledge. https://doi.org/10.4324/9781315661551/ISRAEL-COLONIAL-PROJECT-PALESTINE-ELIA-ZUREIK/ACCESSIBILITY-INFORMATION
- Zureik, E. (2016b). Strategies of Surveillance: The Israeli Gaza. Jerusalem Quarterly, 66, 21–31.
- Zureik, E. (2020). Middle East Critique Settler Colonialism, Neoliberalism and Cyber Surveillance: The Case of Israel. Middle East Critique, 29(2), 219–235. https://doi.org/10.1080/19436149.2020.1732043
- Zureik, E., Lyon, D., & Abu-Laban, Y. (2010). Surveillance and control in Israel/Palestine: Population, territory and power. In Surveillance and Control in Israel/Palestine: Population, Territory and Power. https://doi.org/10.4324/9780203845967

CAPTIVE VOICES: **ALGORITHMIC VOICE SURVEILLANCE IN PALESTINE**

SARAH FATHALLAH

Introduction	62
Background and Context	64
Interception and Capture of Voice Data	73
Voice Data Storage and Retention	78
Voice Data Processing and Analysis	82
Applications for Voice Data	87
Limitations of Algorithmic Voice Techniques	90
Impacts on Palestinians	92
Potential Avenues for Contestation	94
Conclusion	100

Sarah is a community organiser, critical AI researcher, and MSt candidate in AI Ethics and Society at the University of Cambridge. Sarah's scholarship explores the carceral impacts of technology and how artificial intelligence supports the surveillant, experimental, and necropolitical logics of carceral geographies, especially along racialised lines. Her work spans reproductive justice, labor rights, and refugee displacement.

Sarah's fellowship research examines the weaponisation of AI in Israel's surveillance and digital domination of Palestinians, particularly through voice surveillance, capture, and biometric voiceprinting. She investigates whether Israel is building a searchable voice database of Palestinians and identifies the systems and infrastructures enabling this apparatus.



INTRODUCTION

For Palestinians under Israeli occupation, the voice has been weaponized into one of the world's most sophisticated systems of mass surveillance, transforming the very act of speaking to an act of capture. The title, «Captive Voices,» reflects this act: Palestinian voices are captured through interception of communications, captured through algorithmic analysis, and ultimately captured within a system of control that seeks to contain every utterance as potential evidence or justification. This report exposes the architecture of algorithmic voice surveillance in Palestine, revealing how the intimate act of speaking has been transformed into a digital weapon of occupation.

Why voice surveillance matters

Israel's voice-surveillance regime has been described as "one of the world's largest and most intrusive collections of surveillance data over a single population group."[1] Yet despite this scale, public debate has focused far more on CCTV camera surveillance, facial recognition systems, and social media monitoring in Palestine.[2] Indeed, civil society has mobilized forcefully against facial recognition. In 2023, 7amleh, alongside more than 170 civil society organizations—including Amnesty International, Human Rights Watch, and the Internet Freedom Foundation—called for a global ban on facial recognition technologies.[3] Similarly, much has been written about the surveillance of Palestinians' online behavior, and their impacts on their digital rights.[4]

Voice-based communications and surveillance modalities, however, have attracted comparatively little scholarly and public scrutiny. When attention does arise, it tends to emphasize the technical limitations of AI voice technologies in commercial contexts,[5] rather than their role in the policing and the carceral governance of an entire population.

Scope of this report

This reports recognizes "sonic" or "acoustic surveillance" as a broader form of monitoring that concerns the capture of all sounds, as is the case with

1 Yuval Abraham, 'Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians', +972 Magazine, 6 August 2025, https://www.972mag.com/microsoft-8200-intelligence-surveillance-cloud-azure/.

2 7amleh, Intensification of Surveillance in East Jerusalem Since October 2023 (7amleh – The Arab Center for the Advancement of Social Media, 2024), https://7amleh.org/post/surveillance-and-digital-rights-violations-in-east-jerusalem-en; Sophia Goodfriend, The Expansion of Digital Surveillance in Jerusalem and Impact on Palestinians Rights (7amleh – The Arab Center for the Advancement of Social Media, 2021), https://7amleh.org/storage/Digital%20Surveillance%20Jerusalem_7.11.pdf; 7amleh, Facial Recognition Technology and Palestinian Digital Rights (7amleh – The Arab Center for the Advancement of Social Media, 2020), https://7amleh.org/post/facial-recognition-technology-and-palestinian-digital-rights.

3 Amnesty International, Amnesty International and More than 170 Organisations Call for a Ban on Biometric Surveillance, 7 June 2021, https://www.amnesty.org/en/latest/press-release/2021/06/amnesty-international-and-more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/.

4 Eyad Barghuthy and Alison Carmel, Silenced Networks: The Chilling Effect among Palestinian Youth in Social Media (7amleh – The Arab Center for the Advancement of Social Media, 2019), https://7amleh.org/post/silenced-net-the-chilling-effect-among-palestinian-youth-in-social-media; 7amleh, Aš-Šabāb al-Filis□yniyn Wa-Lmušārka Ās-Syāsya □abra Šabakāt at-Ttawā□ul ā-L□ijtimā□y الشباب الفلسطينيين والمشاركة السياسية عبر شبكات التواصل الاجتماعي [Palestinian Youth and Political Participation via Social Media Networks] (7amleh – The Arab Center for the Advancement of Social Media, 2019), https://7amleh.org/wp-content/uploads/2019/10/-1استطلاع-حملة.pdf.

5 Daniel Leufer, 'Sonic Surveillance: Why You Don't Want AI Snooping on You', Access Now, 23 September 2025, https://www.accessnow.org/ai-snooping/.

detecting gunfires[6] or measuring urban noise pollution.[7] The report also understands "digital surveillance" as a broad category that includes tracking online behavior, but does not necessarily focus on the tracking of spoken communications.

More specifically, this report focuses on voice surveillance: the monitoring, interception, and analysis of voice communications, including cellular-based phone calls, which are traditional mobile-network calls tied to phone numbers, and voice over IP (VoIP) communications such as messaging-app calls and voice notes, which are transmitted over the internet and tied to app accounts rather than numbers. The report also covers the associated metadata that provides context to the voices—when they were spoken, by whom, where, and through which devices.

This report also focuses on Palestinians in the occupied territories: the West Bank, East Jerusalem, and Gaza. Palestinian refugees in the diaspora or refugee camps and Palestinian citizens of Israel fall outside this report's scope, though extensive scholarship (in the work of Ahmad H. Sa'di[8], Elia Zureik,[9] and others[10]) addresses the latter context.

Methodology

Investigating surveillance technologies in Palestine requires working against deep institutional secrecy, as information about Israeli surveillance and military operations is extremely difficult to access. This report, nonetheless, aims to gather the limited knowledge that is currently publicly available from public sources, media reporting, and civil society documentation, predominantly in the English and Arabic languages.

Given the opacity surrounding surveillance infrastructures, the report's approach follows the tradition of what epistemologists describe as 'scavenging as a methodology:' piecing together fragments when full empirical evidence is not available. Scavenging as a methodological stance is thus "an adaptive response to scarcity,"[11] one that invokes resourcefulness in the face of withheld or denied information.[12]

This report does not claim to present the full picture of Israel's voice-surveillance architecture. Instead, it offers a partial but critical reconstruction that assembles the puzzle pieces that can be accessed, and that, when placed together, are enough to show how an entire population's spoken words are mined by one of the most pervasive mass surveillance systems in the world.

6 Electronic Frontier Foundation, 'Gunshot Detection', Street Level Surveillance, n.d., https://sls.eff.org/technologies/gunshot-detection.

7 Alaina Demopoulos, 'Honk Honk! Can Noise Cameras Reduce "Potentially Fatal" Sound Pollution?', The Guardian (New York), 4 October 2023, https://www.theguardian.com/us-news/2023/oct/04/new-york-noise-cameras.

8 Ahmad H. Sa'di, Thorough Surveillance: The Genesis of Israeli Policies of Population Management, Surveillance and Political Control towards the Palestinian Minority, Manchester International Relations (Manchester University Press, 2016).

9 Elia T. Zureik, Israel's Colonial Project in Palestine: Brutal Pursuit, Routledge Studies on the Arab-Israeli Conflict 20 (Routledge, 2016).

10 Usama Halabi, 'Legal Analysis and Critique of Some Surveillance Methods Used by Israel', in Surveillance and Control in Israel/Palestine: Population, Territory, and Power, ed. Elia Zureik et al., Routledge Studies in Middle Eastern Politics 33 (Routledge, 2011), https://doi.org/10.4324/9780203845967.

11 Sophie Marie Niang, 'In Defence of What's There: Notes on Scavenging as Methodology', Feminist Review 136, no. 1 (2024): 53, https://doi.org/10.1177/01417789231222606.

12 Niang, 'In Defence of What's There', 57.

1. BACKGROUND AND CONTEXT

1.1. HISTORICAL AND ANALYTICAL GROUNDING

Israel's voice surveillance apparatus cannot be understood in isolation from its historical context and the broader ecosystem of surveillance technologies that constitute the occupation. This historical and analytical grounding reveals how voice surveillance functions not as an isolated technological program, but as an integral component of a comprehensive system of population control.

The historical roots and continuity of Israeli surveillance

Surveillance in Palestine did not begin with the digital age, nor even with the establishment of Israel. In the words of scholar Helga Tawil-Souri, "Zionism was born as a surveillance regime."[13] The roots of Israeli surveillance stretch back to the pre-1948 period, when Zionist militias developed espionage services as auxiliaries to the British police and army, penetrated communication networks, and experimented with wireless interception and cryptography. What would later be formalized as 'Signals Intelligence'—wiretapping, encryption, decryption, and electronic monitoring—was already embedded in the political project that preceded the formation of Israel.[14]

Building on these early collaborations with the British Mandate, Zionist groups systematically collected intelligence on land, population, and social networks. As Tawil-Souri notes, they "learned and benefited from the British Mandate authorities' hordes of documents that detailed and quantified myriad aspects of daily life in Palestine," including tax lists, land surveys, and cadastral maps.[15] One such group, the Shai, conducted the massive "Operation Arab Village," gathering extensive data on villagers, resources, infrastructure, weapons, and even fighters during the 1936-1939 Revolt.[16] This early emphasis on surveillance laid the groundwork for Israel's post-1948 security architecture. For instance, present-day entities like the Shin Bet, Israel's domestic security service overseen by the Prime Minister, evolved directly from these pre-state information-gathering networks,[17] institutionalizing a regime that is not confined to specific targets but is instead expansive and population-wide.

The panoply of surveillance

Importantly, these pre-1948 techniques demonstrate remarkable persistence until today. Israel's current surveillance system still leverages traditional tactics that include "a police force, intelligence agents, informants, spies, infiltrators, collaborators, imprisonment, torture and interrogation methods,

13 Mohammed R. Mhawish, 'Watched, Tracked, and Targeted', New York Magazine, 3 December 2025, https://nymag.com/intelligencer/article/watched-tracked-targeted-israel-surveillance-gaza.html.

14 Helga Tawil-Souri, 'Israel's Telecommunications Lines and Digital Surveillance Routes', in Decolonizing the Study of Palestine: Indigenous Perspectives and Settler Colonialism after Elia Zureik, ed. Ahmad H. Sa'di and Nur Masalha (I.B. Tauris, 2023), 214–15.

15 Helga Tawil-Souri, 'Surveillance Sublime: The Security State in Jerusalem', Jerusalem Quarterly, no. 68 (December 2016): 58, https://doi.org/10.70190/jq.168.p56.

16 Tawil-Souri, 'Surveillance Sublime', 58.

17 Tawil-Souri, 'Surveillance Sublime', 58.

observation from a distance and direct observation, differentiated infrastructure, territorial mapping, land surveys and registration, urban planning, architecture, watch towers, population registration, censuses, identification papers, and slightly newer low-tech tools such as postal interception, wiretapping, and x-ray machines."[18] And even though Israel has increasingly adopted new surveillance technologies—"such as drones, remote controlled robots, biometric data collection, and computer viruses"—those tools "do not displace low-tech ones, but supplement them,"[19] demonstrating that surveillance in Israel is not simply a product of the advent of digital technologies, but a long-standing, hybrid, and all-encompassing regime.

A substantial body of scholarship documents Israel's panoply of surveillance. As the late Elia Zureik notes, surveillance in Israel "extends from the use of methods such as the electronic recording of information through telephone tapping and intercepting electronic messaging."[20] Adding to telecommunications interception and surveillance are biometric and facial recognition systems, physical infrastructure surveillance embedded in checkpoints and urban spaces, drones, digital content monitoring of social media and other online activity, movement and ID control, human informant and collaborator networks, and more.[21]

Voice surveillance, despite being the sole focus of this report, must be understood as one component within an interconnected surveillance ecosystem. Voice surveillance does not operate in isolation but amplifies and is amplified by other surveillance methods. For example, intercepted voice communications may provide information that enables more targeted social media monitoring, while data from facial recognition systems can be cross-referenced with voiceprints to create more comprehensive biometric profiles. This interconnectedness creates a regime where multiple methods reinforce each other to achieve complete population control and resistance suppression, embedding surveillance to the very fabric of the occupation itself.

The algorithmic turn in voice surveillance

The massive repository of stored spoken audio collected from Palestinians is only as valuable as Israel's capacity to process and search the information it contains. Whereas, in the 1990s, Israel relied on human experts to verify the identity of individuals involved in a phone conversation,[22] the sheer volume of voice data amassed today suggests Israel's likely reliance on machine learning and algorithmic tools, not just of speaker identification but more broadly of "knowledge discovery in databases."[23]

18 Tawil-Souri, 'Surveillance Sublime', 59.

19 Tawil-Souri, 'Surveillance Sublime', 59.

20 Elia Zureik, 'Colonialism, Surveillance, and Population Control', in Surveillance and Control in Israel/Palestine: Population, Territory, and Power, ed. Elia Zureik et al., Routledge Studies in Middle Eastern Politics 33 (Routledge, 2011), 12–13, https://doi.org/10.4324/9780203845967.

21 IMEU, Fact Sheet: Israeli Surveillance & Restrictions on Palestinian Movement (Institute for Middle East Understanding, 2021).

22 Dan De Luce, 'Wigs, Robotic Guns and Exploding Pagers: Israel Has a Long History of Hunting down Its Enemies', NBC News, 20 September 2024, https://www.nbcnews.com/investigations/israel-long-history-targeted-killings-enemies-rcna171888.

23 Usama Fayyad et al., 'From Data Mining to Knowledge Discovery in Databases', AI Magazine, 15 March 1996.

it is important to note that such technologies did not emerge suddenly nor recently. According to sources cited by The Guardian, Unit 8200 has "for almost a decade" deployed AI systems to analyze intercepted and stored communications, using "smaller-scale machine learning models" in order "to sort information into predefined categories, learn to recognise patterns and makepredictions."[24]

There is also precedent demonstrating Israel's capacity for advanced voice analysis. Although the exact tools were not named, surveillance scholars Elia Zureik and David Lyon researchers noted the sweeping monitoring powers granted to the Shin Bet and the police during the COVID-19 pandemic.[25] Similarly, researcher Avi Marciano commented on the militaristic framing adopted by authorities, further quoting the Prime Minister who, during a press conference, stated that the same digital tools used on Palestinians were then being used on Israelis for tracking the spread of the virus.[26] Civil society organisations, including 7amleh, warned of the "monitoring and tracking people 24 hours a day, 7 days a week"—including their calls—legitimated "under the pretext of preventing the transmission and spread of infection." [27]

Of particular interest is a form of analysis that enables the identification of individuals based on their voice. In an article by Reuters reporting on a Ministry of Defense-led COVID-19 voice-test study, samples from patients' voices were analyzed using machine-learning algorithms designed to identify unique vocal markers and determine a "vocal fingerprint" for remote diagnosis and monitoring. While unrelated to intelligence operations, the study illustrates that Israel possesses the technical capacity to conduct large-scale, algorithmic voice analysis.[28] These precedents help situate the current infrastructure for processing intercepted audio. They provide important context for understanding the tools likely used by Israel to analyze voice-surveillance data at scale.

Digital occupation

The 1967 occupation ushered in a period where Israel's economy increasingly shifted toward advanced communications technologies, while Palestinians were denied meaningful development of their telecommunications infrastructure, and lived under "a strict military regime limiting most forms of communication from newspapers to fax machines."[29] By the 1990s, Israel continued to invest heavily in its own telecommunications and surveillance architecture, while Palestinian areas remained infrastructurally

24 Harry Davies and Yuval Abraham, 'Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data', The Guardian (Jerusalem), 6 March 2025, https://www.theguardian.com/world/2025/mar/06/israel-military-ai-surveillance.

25 Elia Zureik and David Lyon, 'Coronavirus Surveillance and Minority Groups in Israel/Palestine', The Middle East International Journal for Social Sciences 3, no. 3 (2021): 197–215.

26 Avi Marciano, 'Israel's Mass Surveillance during COVID-19: A Missed Opportunity', Surveillance & Society 19, no. 1 (2021): 85–86, https://doi.org/10.24908/ss.v19i1.14543.

27 7amleh, Netanyahu Imposes Dangerous "Big Brother" Surveillance under the Pretext of a Security Response to the Coronavirus, 23 March 2020, https://www.apc.org/en/news/7amleh-netanyahu-imposes-dangerous-big-brother-surveillance-under-pretext-security-response.

28 Reuters, 'Israeli Defense Ministry Launches COVID-19 Voice-Test Study', Reuters (Jerusalem), 24 March 2020, https://www.reuters.com/article/world/israeli-defense-ministry-launches-covid-19-voice-test-study-idUSKBN21B2YU/.

29 Tawil-Souri, 'Israel's Telecommunications Lines and Digital Surveillance Routes', 215–16.

underdeveloped and easily monitored.[30] As Tawil-Souri articulated, Palestinians were, in effect, "telecommunicatively contained."[31]

The 1993 Oslo Accords period did little to reverse these conditions. At the time, fewer than 2% of Palestinian households had fixed phone lines, contrasting with nearly 75% of Israeli households. The infrastructure transferred to the Palestinian Authority was degraded, and Paltel—established in 1995 to manage telecommunications—struggled to meet demand due to structural constraints such as not having control over the infrastructure, the need for said infrastructure to maintain compatibility with the Israeli framework, and the requirement that equipment acquisitions "be pre-approved by Israel and in certain cases brought from Israeli suppliers."[32] These dependencies obstruct the ability for the Palestinian information and communication technology (ICT) to achieve self-sufficiency. As the Palestinian policy network Al-Shabaka noted, Israel's "severe restrictions on the Palestinian sector" have increased dependence on Israeli systems and undermined Palestinian sovereignty.[33]

This history forms the backbone of what Helga Tawil-Souri terms "digital occupation," describing the enclosures delineated by Israel's limitations and restrictions of "bandwidth; the placement, number, and strength of Internet routers or telephone exchanges; the range of cellular signals; and the equipment used."[34] Experts agree that any actor with the power to "cut off individual users, specific communication services, or entire communities," from digital ecosystems wields significant gatekeeping power.[35] For Palestinians, that actor is Israel. Since October 2023, internet and telecommunications infrastructure in Gaza—including cell towers, cables, servers, and the offices of both Palestinian telecommunications companies—has been deliberately targeted. These attacks, coupled with Israel's ongoing ability to control Palestinian digital infrastructure, caused an unprecedented internet blackout, cutting Gaza's connectivity by over 80%.[36] In the face of this large-scale destruction, it becomes evident that Israel-imposed infrastructural scarcity, dependency, and vulnerability persist to this day.

Digital occupation is not merely a descriptive term for Israel's control over telecommunications infrastructure; it is intrinsically tied to voice surveillance. Older, deliberately limited systems are easier "to limit, control and surveil, whether in terms of eavesdropping, detecting and monitoring data traffic, or the ability to shut it down."[37] Equipment that must pass through Israeli customs or be purchased from Israeli providers may be modified or

30 Tawil-Souri, 'Israel's Telecommunications Lines and Digital Surveillance Routes', 216.

31 Tawil-Souri, 'Israel's Telecommunications Lines and Digital Surveillance Routes', 217.

32 Tawil-Souri, 'Israel's Telecommunications Lines and Digital Surveillance Routes', 217.

33 Helga Tawil-Souri, 'Hacking Palestine: A Digital Occupation', Al Jazeera, 9 November 2011, https://www.aljazeera.com/opinions/2011/11/9/hacking-palestine-a-digital-occupation.

34 Helga Tawil-Souri, 'Digital Occupation: Gaza's High-Tech Enclosure', Journal of Palestine Studies 41, no. 2 (2012): 28, https://doi.org/10.1525/jps.2012.XLI.2.27.

35 Sofie Flensburg and Signe Sophus Lai, 'Follow the Data! A Strategy for Tracing Infrastructural Power', Media and Communication 11, no. 2 (2023): 323, https://doi.org/10.17645/mac.v11i2.6464.

36 Zaha Hassan and H. A. Hellyer, Suppressing Dissent: Shrinking Civic Space, Transnational Repression and Palestine-Israel (Oneworld Academic, 2024), 144–45.

37 Tawil-Souri, 'Israel's Telecommunications Lines and Digital Surveillance Routes', 219.

retrofitted to facilitate surveillance.[38] Because Palestinian networks are dependent on and ultimately routed through Israeli infrastructure, Israel retains the possibility "of tracking, capturing and recording all voice and data traffic, uses and patterns."[39] Israel's global position in sensor engineering, encryption, and signal processing is inseparable from the infrastructures of digital domination it built through occupation.[40]

The everyday, intrusive violence of surveillance

Researchers Nadera Shalhoub-Kevorkian and Abeer Otman show how Israeli surveillance has moved from overt intelligence-gathering to a particular form of monitoring that "is used by the Israeli state to infiltrate and control the daily lives of Palestinians and [their] most intimate aspects—the family and home."[41] Palestinians scholars speak to the everydayness[42] and quotidianness[43] of carceral technologies of surveillance, in that they allow for "the intrusion into homes and communications."[44] Voice surveillance, which captures conversations between family members and loved ones in their homes and communities, is one of the clearest encroachments into these relational spaces.

The pervasive nature of voice surveillance has intimate reverberations inside Palestinians' private lives and communities. Veteran Israeli soldiers have described widespread monitoring of private or intimate conversations, with seemingly "no limits as to what soldiers do with the conversations they have intercepted."[45] He went on to add that "soldiers save the conversations and send them to their friends," signaling that privacy is trivialized amongst those who have access to voice-surveillance data. This is in line with the voice-surveillance project as a whole: in a carceral system of total population control, privacy is not only effectively impossible, but not incompatible with the need for knowability of Palestinians under occupation.

38 Tawil-Souri, 'Israel's Telecommunications Lines and Digital Surveillance Routes', 219.

39 Tawil-Souri, 'Israel's Telecommunications Lines and Digital Surveillance Routes', 219.

40 Tawil-Souri, 'Israel's Telecommunications Lines and Digital Surveillance Routes', 220.

41 Nadera Shalhoub-Kevorkian and Abeer Otman, 'Secrecy as Colonial Violence: The Case of Occupied East Jerusalem', in Decolonizing the Study of Palestine: Indigenous Perspectives and Settler Colonialism after Elia Zureik, ed. Ahmad H. Sa'di and Nur Masalha (I.B. Tauris, 2023), 188, Secrecy as Colonial Violence.

42 Nadera Shalhoub-Kevorkian, Security Theology, Surveillance and the Politics of Fear, 1st edn (Cambridge University Press, 2015), 27, https://doi.org/10.1017/CBO9781316159927.

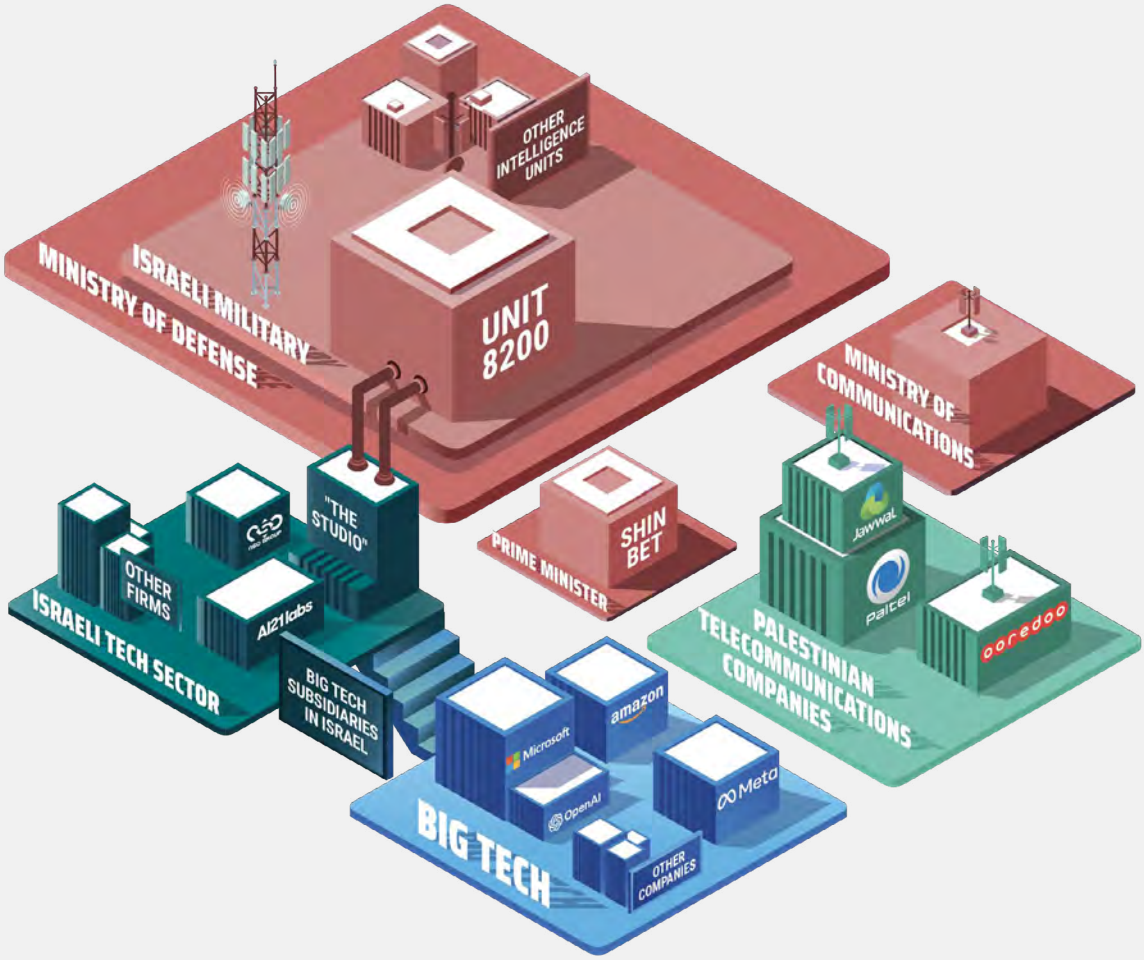
43 Zureik, Israel's Colonial Project in Palestine, 109.

44 Rajaie Batniji, 'Searching for Dignity', The Lancet 380, no. 9840 (2012): 466, https://doi.org/10.1016/S0140-6736(12)61280-X.

45 Lubna Masarwa, 'Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source', Middle East Eye (Jerusalem), 15 November 2021, https://www.middleeasteye.net/news/israel-can-monitor-every-telephone-call-west-bank-and-gaza-intelligence-source.

1.2. ACTORS INVOLVED IN VOICE SURVEILLANCE

Building on the historical and analytical foundations above, it is crucial to identify the actors who collectively shape the voice-surveillance regime in Palestine, shown at a glance in the graphic below. They span state agencies, private Israeli firms, multinational technology companies, and Palestinian telecommunications providers operating under Israeli control.



Israeli government and military

At the very core of the voice-surveillance architecture is Unit 8200, the Israeli army's signals intelligence unit and the largest unit in the Israeli military.[46] Unit 8200 is the primary actor surveilling Palestinian voice communications, intercepting and recording their calls, storing their audio files, and processing and analyzing their data, with the technical help and tools of private companies.

46 Privacy International, The Global Surveillance Industry (2016), 23, https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.

Its work is complemented by the Shin Bet, who holds legal authority to access telecommunications data from Israeli telecommunications companies,[47] and is one of the main recipients of voice data, making it another central actor in the voice-surveillance apparatus.

Another critical actor is the Israeli Ministry of Communications, which directly controls the Palestinian ICT infrastructure. Under its management is the entire cellular spectrum, and "it is Israel's Communication Ministry that determines how much bandwidth" is allowed.[48] Additionally, Palestinians who need to acquire ICT equipment "are required to get approval from the Israeli Ministry of Communications for each shipment they have,"[49] and the Palestinian network must be integrated with the Israeli network, ensuring that it "is compatible with the standards adopted and applied in Israel by the Ministry of Communications."[50]

Israel's private tech sector

Israel's private surveillance sector is so expansive that the country is now the most densely concentrated per capita in the world in numbers of surveillance companies,[51] forming a large-scale data extractive economy.[52] Israel's military surveillance capacity is strengthened by this private tech industry, thanks to a strong "coordination between the Defense Ministry and [...] civilian companies."[53] A key manifestation of this collaboration is "The Studio," a hub within Unit 8200. According to news reporting, many AI-based surveillance tools were developed there by linking active-duty soldiers with reservists employed at tech companies, who contributed "know-how and access to key technologies that weren't available in the military."[54]

A 2016 report from Privacy International taking stock of the state of surveillance globally, including a case study specific to Israel, enumerated at least one actor in audio surveillance, 15 actors in phone monitoring, and more than a dozen others in other technologies that could be relevant to a voice-surveillance apparatus such as internet monitoring and intrusion (the installation of spyware into communication devices).[55] Known Israeli companies that actively market their voice surveillance, biometrics and related analytics technologies include Corsound AI, Cognyte, MultiKol, Nemesysco, NiCE, PerSay, Verint, as well as spyware companies like Candiru, Cellebrite, Cytrox, and Paragon.

47 Euro-Med Human Rights Monitor, Israeli Telecom Companies Must Adhere to UN Principles, Stop Fully Cooperating with Security Agencies, 13 November 2022, https://euromedmonitor.org/en/article/5437/Israeli-telecom-companies-must-adhere-to-UN-principles,-stop-fully-cooperating-with-security-agencies.

48 Tawil-Souri, 'Digital Occupation', 33–35.

49 Wassim F. Abdullah and Sam Bahour, ICT: The Shackled Engine of Palestine's Development (Al-Shabaka, 2015), 7, https://al-shabaka.org/briefs/ict-the-shackled-engine-of-palestines-development/?generate_pdf=view.

50 Xavier Stephane Decoster et al., The Telecommunication Sector in the Palestinian Territories: A Missed Opportunity for Economic Development, no. 104263 (World Bank Group, 2016), 61, http://documents.worldbank.org/curated/en/993031473856114803.

51 Privacy International, The Global Surveillance Industry, 23.

52 Sarah Fathallah and Nick Mitchell, 'Occupied Assets: Israeli Neoliberalism and the Datafication of Palestinian Life', Disjunctions Magazine, January 2026, https://disjunctionsmag.com/articles/occupied-assets/.

53 Abraham, 'Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians'.

54 The Times of Israel, 'Israel Using AI to Pinpoint Hamas Leaders, Find Hostages in Gaza Tunnels — Report', The Times of Israel, 26 April 2025, https://www.timesofisrael.com/israel-using-ai-to-pinpoint-hamas-leaders-find-hostages-in-gaza-tunnels-report/.

55 Privacy International, The Global Surveillance Industry.

Foreign tech companies

Multinational firms—such as Microsoft and Amazon—play essential roles by providing cloud storage and artificial intelligence (AI) services through large government contracts like Project Nimbus.[56] Tech giants also have subsidiaries, research and development centers, and server infrastructures in Israel,[57] which have also proven to be essential in the technical and operational architecture of Israel's voice-surveillance project.

Palestinian telecommunications providers

Finally, Palestinian telecom companies—Jawwal and Ooredoo Palestine—function within a system of Israeli control over spectrum, infrastructure, and equipment imports. As discussed previously, this dependency enables Israeli authorities to monitor, filter, and intercept Palestinian cellular network-based voice communications. It is worth noting that this dependency is in direct violation of the Oslo accords,"[58] which calls for refraining "from any action that interferes with the communication and broadcasting systems and infrastructures of the other side."[59]

1.3. FOLLOWING THE (VOICE-SURVEILLANCE) DATA

Having mapped the actors involved, the next step to understanding Israel's voice-surveillance apparatus requires following the movement of voice data, from capture to usage. This approach draws on a framework outlined by researchers Sofie Flensburg and Signe Sophus Lai, which proposes that, just as investigations of power structures and business systems often 'follow the money,' studies of digital political economies should 'follow the data.'[60] Doing so reveals how collaborations and interdependencies are exercised, maintained, and amplified in data infrastructures, throughout access networks, backbone systems, applications, and data services.[61]

Applying this lens to Palestine allows us to trace how voice communications move from ordinary conversations into the hands of a web of surveillance actors, the relationships between which are visually represented in the map below, and investigated in more detail in the following sections.

56 Al Jazeera, 'What Is Project Nimbus, and Why Are Google Workers Protesting Israel Deal?', Al Jazeera, 23 April 2024, https://www.aljazeera.com/news/2024/4/23/what-is-project-nimbus-and-why-are-google-workers-protesting-israel-deal.

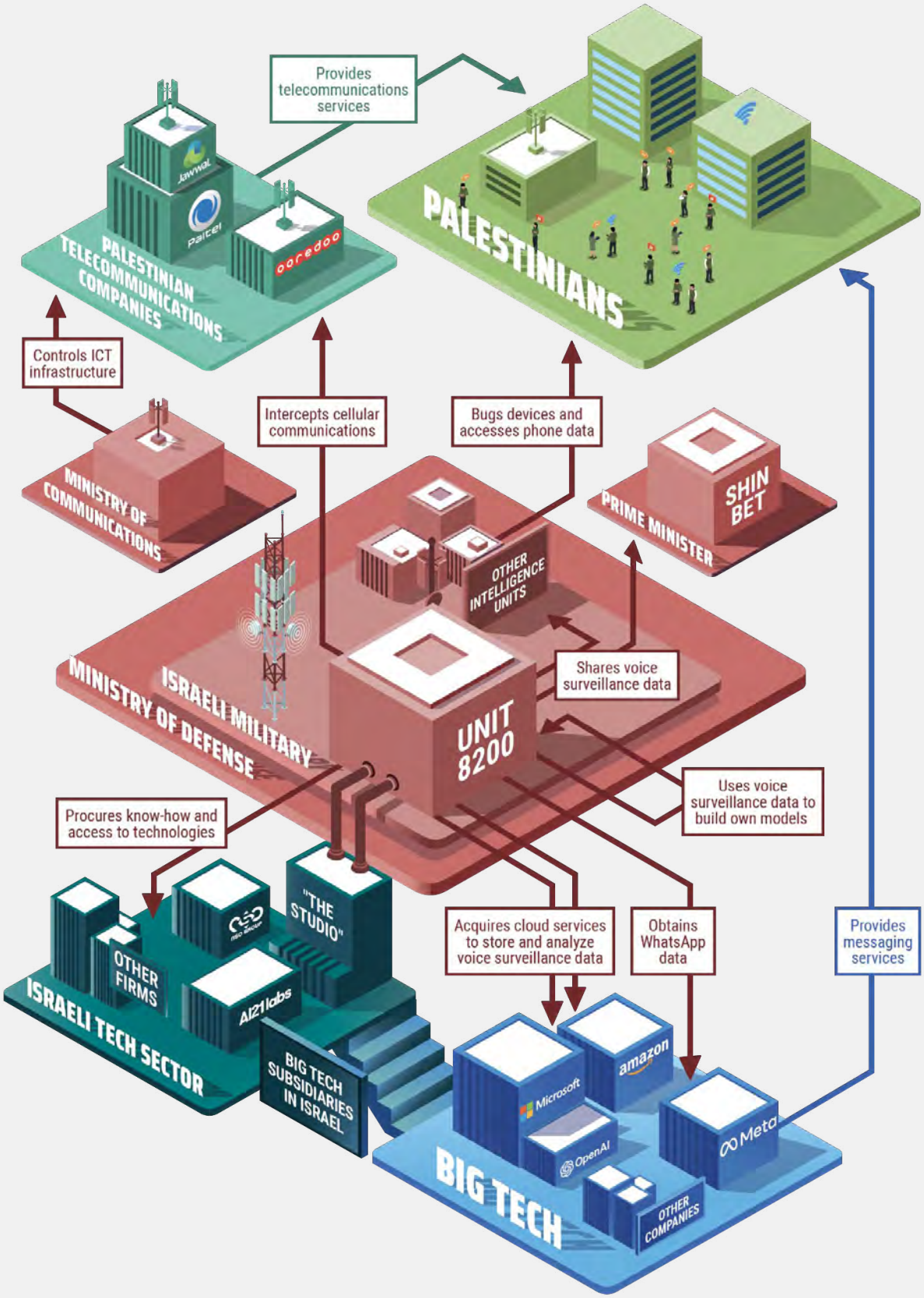
57 Investigate, 'Amazon.Com Inc.', The American Friends Service Committee, 7 August 2024, https://investigate.info/company/amazon; Investigate, 'Microsoft Corp.', The American Friends Service Committee, 29 January 2025, https://investigate.info/company/microsoft.

58 Danny O'Brien and Jillian C. York, 'A Slow Boat to Fast Data: Why Is Palestine Still Waiting for 3G?', Electronic Frontier Foundation, 11 November 2015, https://www.eff.org/deeplinks/2015/11/palestine-3g.

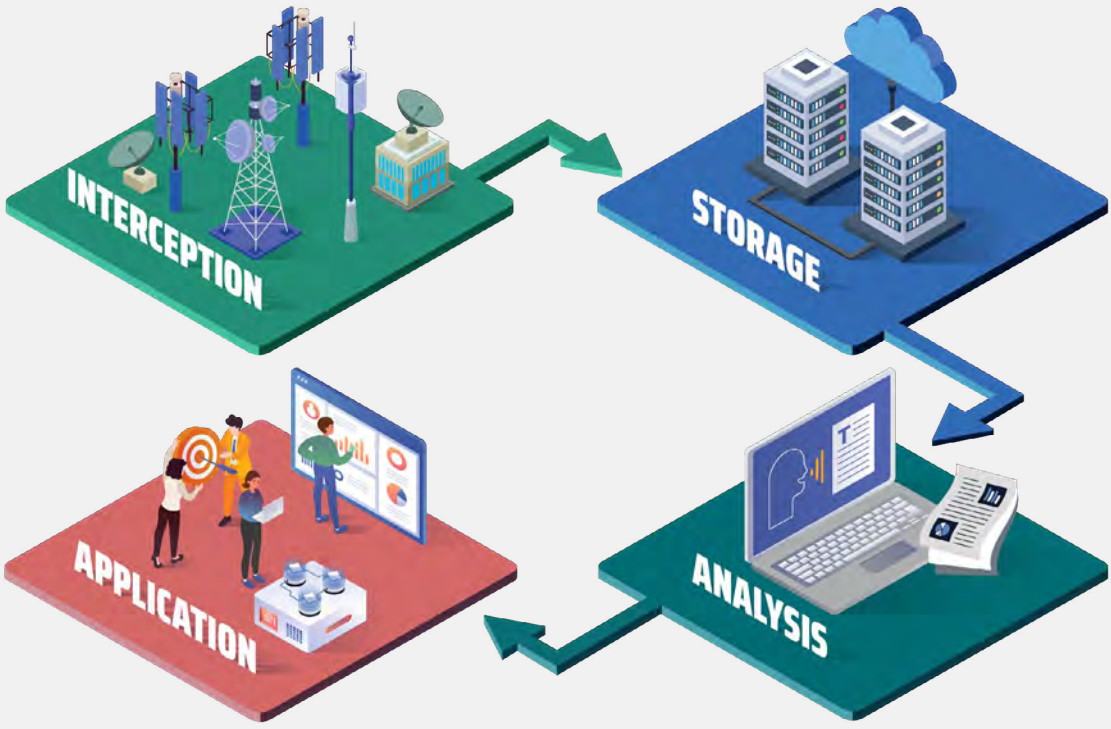
59 Oslo Accords, Annex III, Concerning Civil Affairs, Israeli Palestinian Interim Agreement on The West Bank and the Gaza Strip (Oslo II) (1995), 35–36, https://www.peaceagreements.org/media/documents/ag985_56017411a3c68.pdf.

60 Flensburg and Lai, 'Follow the Data! A Strategy for Tracing Infrastructural Power', 319.

61 Flensburg and Lai, 'Follow the Data! A Strategy for Tracing Infrastructural Power', 319–20.


Provides telecommunications services
PALESTINIANS
PALESTINIAN TELECOMMUNICATIONS COMPANIES
Jawwal
Paltel
ooredoo
Controls ICT infrastructure
Intercepts cellular communications
Bugs devices and accesses phone data
MINISTRY OF COMMUNICATIONS
PRIME MINISTER
SHIN BET
OTHER INTELLIGENCE UNITS
ISRAELI MILITARY
MINISTRY OF DEFENSE
UNIT 8200
Shares voice surveillance data
Uses voice surveillance data to build own models
Procures know-how and access to technologies
"THE STUDIO"
OTHER FIRMS
AI21labs
ISRAELI TECH SECTOR
BIG TECH SUBSIDIARIES IN ISRAEL
Acquires cloud services to store and analyze voice surveillance data
Obtains WhatsApp data
Provides messaging services
Microsoft
amazon
OpenAI
Meta
OTHER COMPANIES
BIG TECH

Following the voice-surveillance data, this report is structured along four steps: the interception of communications and voice data capture (Section 2), the storage and retention of voice-surveillance data (Section 3), the processing and analysis of voice-surveillance data (Section 4), and the applications for voice-surveillance data (Section 5). While presented sequentially, these steps are part of a continuous and iterative process, paradigmatic of data infrastructures.



2. INTERCEPTION AND CAPTURE OF VOICE DATA

2.1. PALESTINIANS UNDER VOICE SURVEILLANCE

What began as targeted monitoring of select individuals has expanded into a population-wide voice-surveillance regime. This section describes the current scope of voice surveillance in Palestine, the groups it singles out for closer scrutiny, and its expanding geographic reach.

Mass surveillance of every Palestinian

Israeli voice surveillance of Palestinians today operates at a mass scale, targeting everyone. Journalist Lubna Masarwa in Middle East Eye reported in 2021 that "Israel can listen to any conversation in the West Bank and the Gaza Strip,"[62] elaborating that, "[a]t any given time, hundreds of soldiers are listening to the conversations being conducted."[63] While this article was new to a more English-speaking (and international) readership, years prior in

62 Masarwa, 'Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source'.

63 Masarwa, 'Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source'.

2014, Waji Al-Jaafari in Ma'an News Agency referenced Palestinian officials who reported that Israel monitors all means of communication in Palestine, including through mobile phones and landlines.[64] For instance, Suleiman al-Zuhairi, Undersecretary of the Ministry of Communications and Information Technology, spoke about Unit 8200's apparatus of electronic espionage used for intercepting, among other things, telephone calls.[65]

This ability to surveil every Palestinian, rather than select targets, is enabled by increased access to cloud storage and cloud computing usage. As part of a 2025 investigation of Israel's "ambitious project to store a giant trove of Palestinians' phone calls on Microsoft servers in Europe," The Guardian called this surveillance system "indiscriminate," allowing "intelligence officers to play back the content of cellular calls made by Palestinians, capturing the conversations of a much larger pool of ordinary civilians."[66] Whereas, before these partnerships with cloud computing giants, the Israeli military was only able to store "the calls of tens of thousands of Palestinians" that were predetermined as surveillance targets, and did so on its own internal servers.[67] With access to cloud storage, the Israeli military no longer needed to limit itself to who should be targeted for surveillance.[68]

Particular target groups of interest

That said, within the broader Palestinian population, the same 2021 Middle East Eye article named two categories of individuals as being of particular interest to Israel's military and internal security agencies. These include: (1) Palestinians who are politically active, and (2) individuals whose personal circumstances make them vulnerable to blackmail. These groups of interest build on long-standing precedents. More than a decade ago, veterans of Unit 8200 acknowledged monitoring Palestinian civilians in order to gather sensitive personal information for potential leverage, and also "admitted to tracking political activists."[69]

When it comes to the former group, a human rights lawyer described how the Shin Bet is "particularly bothered by nonviolent activists, because such people can lead a popular movement and generate widespread protest."[70] In his view, "what worries them most is civil society organisations, because they could lead to the end of the occupation and they garner sympathy in the international community."[71] Surveilling politically active Palestinians is central to Israel's resistance suppression aims.

64 Wajdi Al-Jaafari, '"Masʾūlūn: jamy' wasāʾil al'ittiṣāl fī falasṭīn murāqaba" مسؤولون: جميع وسائل الاتصال في فلسطين مراقبة [Officials: All means of communication in Palestine are monitored]', Ma'an News Agency, 20 December 2014, https://www.maannews.net/news/748592.html.

65 Al-Jaafari, '"Masʾūlūn: jamy' wasāʾil al'ittiṣāl fī falasṭīn murāqaba" مسؤولون: جميع وسائل الاتصال في فلسطين مراقبة [Officials: All means of communication in Palestine are monitored]'.

66 Harry Davies and Yuval Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians', The Guardian, 6 August 2025, https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud.

67 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

68 Abraham, 'Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians'.

69 Yuval Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians', +972 Magazine, 6 March 2025, https://www.972mag.com/israeli-intelligence-chatgpt-8200-surveillance-ai/.

70 Masarwa, 'Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source'.

71 Masarwa, 'Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source'.

As for the latter group, whom an Israeli army veteran called "pressure points," it includes people whom or whose family members—for their sexual orientation, illnesses, indebtedness, or other circumstances—are forced by the Shin Bet "to collaborate or reveal things about other people," as a practice of control and intimidation.[72]

Geographic focus and expansion

Geographically speaking, voice surveillance initially focused on the Palestinian population of the West Bank. In recent years, the system expanded to cover Gaza as well.[73] After October 2023, an intelligence officer explained to +972 Magazine that "internal enthusiasm for storing mass surveillance data from Gaza on the cloud-based system increased," stating that the goal was to head "toward long-term control there, like in the West Bank."[74] However, sources expressed to The Guardian their concerns about how this voice-surveillance project might be impacted by the destruction of the telecommunications infrastructure in Gaza,[75] which "has reduced the volume of phone calls in the territory."[76]

The expansion from targeted to population-wide voice surveillance, its geographic extension from the West Bank to include Gaza as well, and the vastly increased collection capacity afforded by cloud infrastructure raise critical questions about what forms of data are being captured.

2.2. DATA CAPTURED

Audio recordings of conversations

Available reporting indicates that the system archives recordings of calls made daily by Palestinians, in the form of audio files—not just textual data,[77] archiving "millions of mobile phone calls made each day by Palestinians in Gaza and the West Bank."[78] These intercepted audio recordings constitute the core of the voice-surveillance repository.

Corresponding metadata

In addition to audio files, the system collects the corresponding metadata linked to each call. While audio files reveal what is being said, metadata gives information about phone call participants, time, as well as contacts and location.[79]

72 Masarwa, 'Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source'.

73 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

74 Abraham, 'Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians'.

75 Mohammed Alshurafa, The Impact of the Gaza Blockade and the Destruction of Telecommunications Infrastructure on the Digital Economy Amidst Genocide (7amleh – The Arab Center for the Advancement of Social Media, 2025), https://7amleh.org/post/gaza-digital-economy-collapse-en; 7amleh, Gaza Telecommunications Infrastructure: Assessment to Damages and Humanitarian Impact (7amleh – The Arab Center for the Advancement of Social Media, 2024), https://7amleh.org/post/impact-of-war-on-gaza-s-telecommunications-infrastructure-en.

76 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

77 Yuval Abraham, '"Order from Amazon": How Tech Giants Are Storing Mass Data for Israel's War', +972 Magazine, 4 August 2024, https://www.972mag.com/cloud-israeli-army-gaza-amazon-google-microsoft/; Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'; Abraham, 'Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians'.

78 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

79 Robin James, 'Acousmatic Surveillance and Big Data', Sounding Out!, 20 October 2014, https://soundstudiesblog.com/2014/10/20/the-acousmatic-era-of-surveillance/.

Voice-surveillance metadata extracted alongside phone calls most likely include the time and duration of the call, the date and time stamps, the source and destination of the call, the participants in the call, the owner of the device or SIM card associated with the call, and more. As described in one report in The Guardian, "intercepted phone calls tied to a person's profile [...] include the time the person called and the names and numbers of those on the call."[80]

Even though metadata provides mainly contextual information around the voice conversation, a lot can be surmised from it about the content of the conversation as well. Lawyer Usama Halabi illustrates this point through an example, stating that, for instance, if the metadata reveals "that a journalist called a certain source, it may be possible to ascertain to a significant degree the content of the call from the mere fact that it was made."[81]

Potential WhatsApp-related data

Reports that surfaced in 2024 hypothesized that the data captured by the voice-surveillance regime may extend beyond traditional telecom calls to include information associated with WhatsApp communications.[82] Observers have raised the possibility that Israel is collecting WhatsApp-related data, though it remains unclear whether this includes only metadata or also the content of communications such as voice notes and in-app call recordings. If accurate, these reports would suggest an even broader sweep of captured data, encompassing both telecom network activity and app-based voice exchanges.

2.3. INTERCEPTION METHODS

Israel's voice surveillance of Palestinians relies on multiple interception methods that draw on both direct access to telecommunications infrastructure and the compromise of individual devices. Two mechanisms—bugging phones and monitoring ICT networks serving the occupied territories—are well documented. A third, still unconfirmed, concerns the possible interception of data from encrypted messaging applications such as WhatsApp.

Compromising devices through implanted bugs and spyware

One confirmed interception method for voice-surveillance data involves the physical compromise of mobile phones entering Gaza. A former signals intelligence member told Middle East Eye in 2021 that "[e]very mobile or phone imported into Gaza through the Kerem Shalom crossing [...] is implanted with an Israeli bug."[83] The use of the term 'implanted' suggests a hardware-based mechanism rather than software-based spyware, indicating the insertion of an electronic component that can transform the phone into

80 Michael Biesecker et al., 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies', AP News (Tel Aviv), 18 February 2025, https://apnews.com/article/israel-palestinians-ai-technology-737bc17af7b03e98c29cec4e15d0f108.

81 Halabi, 'Legal Analysis and Critique of Some Surveillance Methods Used by Israel', 215.

82 Sada Social, Sada Social Calls for Immediate Investigation into Meta's Leak of WhatsApp Users' Data to the Israeli Military, 18 May 2024, https://sada.social/post/sd-soshal-ydaao-l-thkyk-aaagl-ofory-ltsryb-myta-byanat-mstkhdmy-oatsab-l-algysh-alsrayly; Rabia Ali, 'Is WhatsApp Putting Palestinians at Risk of Being Killed in Gaza?', Anadolu, 30 April 2024, https://www.aa.com.tr/en/artificial-intelligence/is-whatsapp-putting-palestinians-at-risk-of-being-killed-in-gaza/3206563; Paul Biggar, Meta and Lavender, 16 April 2024, https://blog.paulbiggar.com/meta-and-lavender/.

83 Masarwa, 'Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source'.

a listening device. This interpretation aligns with earlier statements from former Minister of Communications Masshour Abu Daqqa, who noted in 2014 that Israel prevented the entry of devices—particularly some Chinese equipment—that it found difficult to hack or eavesdrop on,[84] further substantiating the use of hardware-based interception.

Phones can also be compromised through spyware, which can covertly activate a device's microphone and access a broad range of data. One of the most widely known examples is NSO Group ("NSO")'s Pegasus software. Human Rights Watch describes Pegasus as able to turn a phone "into a portable surveillance tool by gaining access to the phone's camera, microphone, and text messages."[85] One instance of the use of Pegasus on Palestinians was corroborated by technical research conducted in 2021 by Front Line Defenders.[86] Their research was later independently peer reviewed by the University of Toronto's Citizen Lab and Amnesty International's Security Lab, who performed forensic analysis and concluded "that the devices of six Palestinian human rights defenders were hacked with NSO's Pegasus spyware in 2020 and 2021."[87]

Controlling telecommunications infrastructure

A second confirmed interception mechanism derives from Israel's structural control over Palestinian telecommunications networks, previously delineated in Section 1. As one source explained to Middle East Eye, "anyone using the only two mobile networks serving the occupied territories [Jawwal and Wataniya—now Ooredoo Palestine] is being monitored."[88]

The Electronic Frontier Foundation noted in 2015 that Israel had restricted Palestinian operators, locking them down to older generations of mobile technology that is "more vulnerable to being tapped," and blocking access to newer systems that "are safer from passive surveillance,"[89] enabling Israel to "surveil and eavesdrop [...] on traffic coming over Israeli companies' networks" without being detected.[90] Without this level of control, Israel would need to resort to more active modes of surveillance, such as using spying technology like IMSI (International Mobile Subscriber Identity) catchers. However, unlike passive surveillance, active surveillance is more detectable.

Possibly accessing WhatsApp communications

A further, though still unresolved, question concerns whether Israel can access communications conducted via WhatsApp, the contents of which are presumably encrypted. Reports by +972 Magazine and Local Call, citing

84 Al-Jaafari, '"Masūlūn: jamy' wasā'il al'ittiṣāl fī falasṭīn murāqaba" مسؤولون: جميع وسائل الاتصال في فلسطين مراقبة [Officials: All means of communication in Palestine are monitored]'.

85 Human Rights Watch, Spyware Used to Hack Palestinian Rights Defenders, 8 November 2021, https://www.hrw.org/news/2021/11/08/spyware-used-hack-palestinian-rights-defenders.

86 Front Line Defenders, OPT/Israel: Six Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware (Front Line Defenders, 2021), https://www.frontlinedefenders.org/en/statement-report/six-palestinian-human-rights-defenders-hacked-nso-groups-pegasus-spyware.

87 Amnesty International, Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware, 8 November 2021, https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/.

88 Masarwa, 'Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source'.

89 O'Brien and York, 'A Slow Boat to Fast Data: Why Is Palestine Still Waiting for 3G?'

90 O'Brien and York, 'A Slow Boat to Fast Data: Why Is Palestine Still Waiting for 3G?'

six Israeli intelligence officers, claim that conversations between Palestinians on WhatsApp have been used to feed Israel's target-generation system, Lavender. The reporting prompted questions from observers, including Tech for Palestine founder Paul Biggar, who asked, "Where are they getting this data? Is WhatsApp sharing it?"[91] On their end, a WhatsApp spokesperson denied that the company provided a backdoor or "bulk information" to any government, implying Israel as well.[92] Nonetheless, a 2024 press release by civil society organization Sada Social Center admonished Meta for what they considered to be a "leak of Palestinian data" that includes their communications via WhatsApp.[93] However, some have suggested that Israel might have obtained WhatsApp data through methods other than backdoor access or a leak. Journalist Marc Owen Jones suggested Israel could gain access to WhatsApp data through other means, such as through informants, hacking, or spyware.[94] This is not a far-fetched hypothesis, seeing as, in October 2025, a United States (U.S.) judge granted Meta an injunction to stop NSO's spyware from targeting WhatsApp users, particularly journalists, lawyers, and human rights activists,[95] an injunction NSO has since sought to overturn.[96] Additionally, other experts like activist Esra'a Al Shafei posited that Israel may have access to "the metadata alone," which, still, would reveal group memberships, contact networks, and communication patterns but not conversation content.[97]

3. VOICE DATA STORAGE AND RETENTION

Israel's mass interception of Palestinian voice communications relies on a layered storage architecture supported by major cloud providers and flexible retention practices. Large volumes of audio recordings and associated metadata are housed across Microsoft Azure and Amazon Web Services (AWS) environments, seemingly both inside Israel and in data centers abroad, reflecting the scale of surveillance and the military's reliance on commercial cloud infrastructure.

3.1. CLOUD STORAGE AND PROVIDERS

The scale and scope of Israel's voice surveillance of Palestinians has made reliance on commercial cloud providers essential. The volume of data—comprising billions of audio files and associated metadata—exceeds what could reasonably be stored on military servers alone. As a result, much of the intercepted voice data is hosted in the cloud, primarily through Microsoft

91 Biggar, Meta and Lavender.

92 Ali, 'Is WhatsApp Putting Palestinians at Risk of Being Killed in Gaza?'

93 Sada Social, Sada Social Calls for Immediate Investigation into Meta's Leak of WhatsApp Users' Data to the Israeli Military.

94 Marc Owen [@marcowenjones] Jones, 'The question about Lavender using Whatsapp groups for their targeting, and Meta's potential role in this is important', 17 April 2024, https://x.com/marcowenjones/status/1780501998728540589?ref_src=twsrc%5Etfw.

95 Al Jazeera, 'US Court Bars Israeli Spyware Firm from Targeting WhatsApp Users', Al Jazeera, 18 October 2025, https://www.aljazeera.com/news/2025/10/18/us-court-bars-israeli-spyware-firm-from-targeting-whatsapp-users.

96 Suzanne Smalley, 'NSO Seeks to Overturn WhatsApp Case, Saying It Is "Catastrophic" for the Spyware Maker', The Record, 20 November 2025, https://therecord.media/nso-seeks-to-overturn-whatsapp-case.

97 Julia Conley, 'Report Indicates Israel Uses WhatsApp Data in Targeted Killings of Palestinians', Truthout, 19 May 2024, https://truthout.org/articles/report-indicates-israel-uses-whatsapp-data-in-targeted-killings-of-palestinians/.

Azure and AWS, with some data reportedly still retained on Israeli military servers, though details about domestic storage remain limited.

Microsoft Azure

Investigations in 2025 by The Guardian, +972 Magazine, and Local Call, drawing on leaked Microsoft documents and interviews with nearly a dozen sources from Microsoft and the Israeli military, revealed that Unit 8200 transferred recordings of Palestinian calls to a "customized and segregated area within Microsoft's Azure cloud platform."[98] This includes voice data from the population of Gaza.[99] The setup of this cloud environment was the result of a close collaboration between Microsoft engineers and Unit 8200, beginning as early as 2022, aiming to create a system "carefully tailored to the unit's needs."[100] Some Microsoft employees involved were themselves former Unit 8200 members, a factor described by sources as making the collaboration "much easier."[101] This collaboration forms part of a broader, privileged partnership between Microsoft and Israel, with the tech giant being examined as having a "footprint in all major military infrastructures inIsrael."[102]

Amazon Web Services

In addition to Microsoft, Amazon also provides cloud storage for Israeli voice-surveillance data. Another investigation by +972 Magazine and Local Call reported that AWS hosts data collected through the mass surveillance of Gaza's population, including billions of audio files.[103] It is unclear whether this storage is part of Project Nimbus—the $1.3 billion joint cloud and artificial intelligence contract signed by Google and Amazon with the Israeli government and military in 2021—though it is known that the majority of purchases from Amazon and Google are carried out through said contract. Similarly to Microsoft, Amazon is, too, considered to have a close partnership with Israel, providing "Israel's Military Intelligence Directorate with a server farm which is used to store masses of intelligence information."[104]

Publicly available reports on Amazon's role seems to indicate that its storing of voice-surveillance data is more focused on the people of Gaza, as said reports do not explicitly mention the West Bank or occupied East Jerusalem. According to multiple sources, the AWS public cloud system allows the Israeli military to have "endless storage" for holding intelligence on almost 'everyone' in Gaza."[105] Although the system had been in use since the end of 2022, its operational role expanded significantly after October 2023.[106]

98 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

99 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

100 Abraham, 'Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians'.

101 Abraham, 'Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians'.

102 Abraham, 'Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians'.

103 Abraham, '"Order from Amazon": How Tech Giants Are Storing Mass Data for Israel's War'.

104 Abraham, '"Order from Amazon": How Tech Giants Are Storing Mass Data for Israel's War'.

105 Abraham, '"Order from Amazon": How Tech Giants Are Storing Mass Data for Israel's War'.

106 Abraham, '"Order from Amazon": How Tech Giants Are Storing Mass Data for Israel's War'.

Reliance on Big Tech's cloud infrastructure

Israeli military sources acknowledge that the scale of its voice-surveillance architecture necessitates reliance on Big Tech cloud providers, as it "is so large that it cannot be stored on military servers alone."[107] In the words of the officer in charge of Israel's Digital Transformation Administration in a 2020 interview, "[t]he army can't compete with the resources that the cloud giants and the rest of the cloud providers invest in building their cloud, so it's useless to even try and compete with them."[108] For this reason, Unit 8200 leadership concluded that Azure's "near-limitless storage capacity" was essential to store the communications of an entire population, and had ambitions to expand this operation significantly—to the tune of "tenfold in thecomingyears."[109]

3.2. LOCATION OF DATA CENTERS AND SERVERS

Recent reporting has shed light on the geographic distribution of the infrastructure used to store Israel's voice-surveillance data on Palestinians. A significant portion of this data—amounting to thousands of terabytes—has been held outside Israel, primarily in Microsoft Azure data centers located in Europe.

European data centers

According to a joint investigation by The Guardian, +972 Magazine, and Local Call, "leaked Microsoft files suggest that a large proportion of the unit's sensitive data may now be sitting in the company's datacentres in the Netherlands and Ireland."[110] By July 2025, Microsoft's Azure facility—a 14-hectare data-center campus near Middenmeer in North Holland—was reportedly hosting 11,500 terabytes of Israeli military data, described as roughly 200 million hours of audio files.[111] In another report by the same investigative team, the volume was cited as "as much as 8,000 terabytes of data,"[112] reflecting some variation in publicly available estimates but still highlighting the immense scale of the voice data stored.

Ireland served as an additional European hub, which is not surprising given that it is home to Microsoft's European headquarters.[113] Although exact figures were not disclosed, reporting indicates that a "smaller proportion" of the total data—relative to the volume held in the Netherlands—was stored in Microsoft Azure servers there.[114]

107 Abraham, '"Order from Amazon": How Tech Giants Are Storing Mass Data for Israel's War'.

108 Josh Mitnick, 'Here's How the Israeli Army Is Embracing Digital Transformation', CIO, 8 February 2020.

109 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

110 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

111 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

112 Harry Davies and Yuval Abraham, 'Microsoft Blocks Israel's Use of Its Technology in Mass Surveillance of Palestinians', The Guardian, 25 September 2025, https://www.theguardian.com/world/2025/sep/25/microsoft-blocks-israels-use-of-its-technology-in-mass-surveillance-of-palestinians.

113 Lisa O'Carroll, 'Irish Authorities Asked to Investigate Microsoft over Alleged Unlawful Data Processing by IDF', The Guardian, 4 December 2025, https://www.theguardian.com/technology/2025/dec/04/irish-authorities-asked-to-investigate-microsoft-over-alleged-unlawful-data-processing-by-idf.

114 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

Rapid data relocation after public exposure

Following publication of the joint investigation detailing these arrangements, Unit 8200 appears to have moved quickly to extract its voice-surveillance archives from at least one European Union (EU) jurisdiction. According to sources familiar with the transfer, the data was relocated "within days," with the move occurring in early August 2025. Intelligence officials suggested that the data was likely being transferred to Amazon Web Services (AWS), which was not confirmed by either Israel's military nor Amazon.[115]

Storage within Israel

In contrast to the details emerging from reporting on European infrastructure, the location and scale of servers inside Israel remain far less visible. Prior to its migration to the cloud, Unit 8200 stored only the calls of those pre-designated as surveillance 'suspects' on its own internal servers.[116] Even before the decision to shift storage from Microsoft's servers in the Netherlands, Unit 8200 allegedly planned to migrate as much as 70% of its voice-surveillance data to Azure,[117] suggesting that at least some of the voice data repository would remain under the unit's storage infrastructure.

It is unclear whether this residual data resides on the military's own servers or in facilities operated within Israel by Microsoft and Amazon. Both companies have expanded their data center infrastructure in the past several years, with Microsoft launching a datacenter region in Israel in 2020[118] and Amazon in 2023.[119] Even so, public sources do not clarify where voice-surveillance data is stored inside Israel.

3.3. DATA RETENTION PERIODS

Israel's retention of intercepted Palestinian voice data remains flexible in practice. According to intelligence sources cited in recent investigations, recorded calls—including those made to international and Israeli numbers—are "typically retained in the cloud for about one month" in the case of Microsoft Azure.[120] However, these same sources emphasized that the retention period can be extended on demand, enabling Unit 8200 to preserve recordings for significantly longer periods "when needed."[121] The Azure-based storage and processing environment is designed to allow officers to "play back and analyse the content of cellular calls of an entire population."[122] This means that intelligence officers can retroactively retrieve the conversations of individuals who later become "of interest," effectively transforming a month-long retention policy into a selective long-term

115 Davies and Abraham, 'Microsoft Blocks Israel's Use of Its Technology in Mass Surveillance of Palestinians'.

116 Abraham, 'Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians'.

117 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

118 Microsoft, Microsoft to Launch New Cloud Data Center Region in Israel, 22 January 2020, https://news.microsoft.com/source/emea/features/microsoft-to-launch-new-cloud-datacenter-region-in-israel/.

119 Dan Swinhoe, AWS Launches Israeli Cloud Region in Tel Aviv, 2 August 2023.

120 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

121 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

122 Davies and Abraham, 'Microsoft Blocks Israel's Use of Its Technology in Mass Surveillance of Palestinians'.

archive.[123] No publicly available information exists on the retention periods for voice-surveillance data stored in Amazon AWS.

4. VOICE DATA PROCESSING AND ANALYSIS

This section details the algorithmic tools likely used to process and analyze voice-surveillance data, specifically to identify speakers, transcribe and translate recorded audio, and analyze the contents of speech.

4.1. SPEAKER IDENTIFICATION

In simplified terms, Israel's ability to identify individuals participating in intercepted calls is likely grounded in two broad methods of speaker identification: metadata-based inference and biometric voiceprinting. Both approaches are not mutually exclusive.

Metadata-based inference

The first method relies on information obtained from telecommunications metadata, particularly the SIM cards used to place or receive a call. By linking the SIM ID to subscriber records, authorities can narrow the pool of likely speakers to the card owner and their immediate family or social network. Even when the speaker is not the registered owner, patterns in their networks and contact lists may allow analysts to deduce who is using the device at any given moment. This method was referenced in an AP News article detailing that intercepted calls "tied to a person's profile also include the time the person called and the names and numbers of those on thecall."[124]

Biometric voiceprinting

The second method, voiceprinting, is a biometric technique that derives a unique vocal signature from an individual's physiological characteristic (e.g., vocal tract shape, glottis, nasal cavity) and behavioural speech patterns (e.g., accent, pitch, speaking style). Researchers at the Palestine Polytechnic University note that voiceprinting has distinct advantages over other biometric modalities, explaining that, a "voiceprint does not require special hardware like a fingerprint sensor or iris-scanning equipment, it just requires a microphone which is cheap and easy to get."[125] Microphones, especially those built in mobile phones, don't even need to be acquired by Israel.

Several recent commentaries—primarily opinion pieces—assert that Israel is deploying voiceprinting at scale. Articles in Al Majalla by foreign-policy analyst Marco Mossad claim that the Israeli military created a "voice

123 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

124 Biesecker et al., 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies', 18 February 2025.

125 Mohamad Ateyyah Salah et al., 'Voiceprint Authentication System' (Palestine Polytechnic University, 2021), https://scholar.ppu.edu/bitstream/handle/123456789/7547/Voiceprint-Authentication-System.pdf.

library,"[126] and tracked militants' calls "through their phones, listened to their calls with relatives and family members, and then recorded each voice, creating their unique voiceprints in databases,"[127] allegedly enabling rapid identification during eavesdropping operations. Similar assertions are made in The Peninsula by cyber-politics researcher Khaled Walid Mahmoud, who describes "massive voice libraries" used to match newly intercepted audio against stored profiles and suggests that system accuracy increases as more calls are captured.[128] Retired Major General Fayez al-Duwairi, in Al Jazeera, further contended that Israel collected the voices of approximately 37,000 individuals at the outset of its recent military campaign in Gaza.[129]

Although these accounts provide a consistent narrative, they do not offer verifiable sourcing. Earlier reporting, however, indicates that such capabilities have been discussed within Palestinian media for over a decade. In 2013, Palestine Today cited security researcher Samir Mahmoud Qaddih who described the use of voiceprints by Israel after tapping the phone calls and tracing the full call histories of targeted individuals and their contacts.[130] Al-Monitor (2014)[131] and Rai Al-Youm (2016) echoed these claims, with the latter adding that device microphones could allegedly capture sound even when phones were switched off,[132] something advanced spyware can achieve by simulating a power-off state to deceive the user while the device remains turned on and under malicious control.[133]

Unresolved questions about technology providers

On the one hand, speaker identification through metadata is likely done by Israeli intelligence units, using data captured through the monitoring of cellular networks, potentially in collaboration with the Israeli Ministry of Communications. This hypothesis is an educated guess.

On the other hand, despite the recurring references to voiceprinting, publicly available information does not clarify whether these systems are developed in-house by the Israeli military, procured from domestic private contractors, or sourced from international vendors. Israel's private sector includes

126 Marco Mossad, 'Are Global Tech Giants Facilitating Israel's War on Gaza?', Al Majalla, 31 May 2024, https://en.majalla.com/node/318176/science-technology/are-global-tech-giants-facilitating-israel%E2%80%99s-war-gaza.

127 Marco Mossad, 'Voiceprint Technology: A Commercial Hit with Military Utility', Al Majalla, 7 February 2024, https://en.majalla.com/node/310146/science-technology/voiceprint-technology-commercial-hit-military-utility.

128 Khalid Walid Mahmoud, 'Voiceprint: From a Verification Tool to a Tracking Technology', The Peninsula, 19 January 2025, https://thepeninsulaqatar.com/opinion/19/01/2025/voiceprint-from-a-verification-tool-to-a-tracking-technology.

129 Al Jazeera, 'Al-Duwairi: Al-Āṯilāl Yastḫdim Baṣmaẗ al-Ṣūt Wālʿīn Litʿqwb Muqātilī al-Muqāwama Biġaza الدويري: الاحتلال يستخدم بصمة الصوت والعين لتعقّب مقاتلي المقاومة بغزة [Al-Duwairi: The Occupation Uses Voice and Eye Scans to Track Resistance Fighters in Gaza]', Al Jazeera, 15 April 2025, https://www.aljazeera.net/news/الدويري-الاحتلال-يستخدم-بصمة-الصوت.

130 Palestine Today, '"Kayfa tatanaʿat ālmuʿābarāt ālʾisrāʾīlya ʿalā jawwālik āšaʿsy!?" كيف تتنصت المخابرات الإسرائيلية على جوالك الشخصي؟! [How does Israeli intelligence eavesdrop on your personal mobile phone?!]', Palestine Today, 30 December 2013, https://paltodaytv.com/post/466/كيف-تتنصت-المخابرات-الإسرائيلية-على-جوالك-الشخصي.

131 Hana Salah, '"Albaṣma as-ṣaūtya" Adāt Isrāʿīl Litanfiʿ Syāsat "Attaʿafya al-Jasadya" "التصفية الجسدية" أداة إسرائيل لتنفيذ سياسة "البصمة الصوتية" ["Voiceprints": Israel's Tool for Implementing "Elimination"]', Al-Monitor, 4 February 2014, https://www.al-monitor.com/ar/contents/articles/originals/2014/02/gaza-israel-islamic-jihad-hamas-mobile-war.html.

132 Yassin Jamil, '"Tafāʿīl Muḫhila ʿan ʿuruq Wa ʿasālīb al-Murāqaba as-Sirrya al-Isrāʿīlya Lil-Hawātif al-Jawwāla Lil-Muqāwama al-Filsʿīnya Wal-Lubnānya" تفاصيل مذهلة عن طرق وأساليب المراقبة السرية الإسرائيلية للهواتف الجوالة للمقاومة الفلسطينية واللبنانية [Shocking Details Emerge about Israel's Covert Methods and Techniques for Monitoring the Mobile Phones of the Palestinian and Lebanese Resistance]', Rai Alyoum, 21 June 2016, https://www.raialyoum.com/ا-تفاصيل-مذهلة-عن-طرق-وأساليب-المراقبة.

133 AVG, Malware Is Still Spying on You Even When Your Mobile Is Off, 14 September 2018, https://www.avg.com/en/signal/android-spyware-that-works-when-your-phone-is-off.

a plethora of companies with advanced audio-analysis capabilities, and Unit 8200 is known to incubate its own technologies. Thus, the provenance of speaker-identification tools remains an open question.

4.2. SPEECH TRANSCRIPTION AND TRANSLATION

Israel's voice-surveillance system necessitates large-scale speech transcription and translation. The first process, speech transcription, is technically referred to as automatic speech recognition (ASR) or speech-to-text (STT)—the two having subtle differences that are not of major relevance for this report and are often used interchangeably. The second process, speech translation, is distinct from speech transcription. However, most available sources discuss them together, and for the purposes of this report, they are therefore treated as a combined set of capabilities for converting spoken Arabic into searchable, analyzable text.

From manual to automated transcription

Historically, intercepted conversations were transcribed manually. Former soldiers have described how Jewish Israeli soldiers who studied Arabic were tasked with listening to recorded calls and producing transcripts.[134] Their work was reviewed by Druze soldiers or Jewish soldiers of Syrian descent, "for whom Arabic is their mother tongue,"[135] as most military officers admitted in testimonials that their level of Arabic is "basically zero."[136] Given, again, the scale of voice-surveillance data being captured by Israel, the processes of transcription and translation are now relying on automated systems.

Rationale for the integration of cloud-based transcription tools

The use of Microsoft Azure's models—along with those of other cloud companies—is accompanied or is potentially supplanting Unit 8200's own "smaller language models" capable of transcribing and translating spoken Arabic to Hebrew.[137] A +972 Magazine recalled internal discussions around cloud migration, explaining that commanders emphasised the advantage of leveraging built-in cloud services once their data is migrated to the cloud, as the cloud service providers "also have their own STT [speech-to-text] capabilities. These are good; they have many capabilities. Why develop everything in the army unit if the capabilities already exist?"[138]

Experts of algorithmic supply chains explain how this is part of the modus operandi of cloud providers. Such companies, as is the case for Microsoft, offer their own pre-built AI technologies as a service "in areas such as language, speech, [...] and analytics," alongside their cloud storage capabilities.[139] Only a limited number of organizations "can produce bespoke

134 Masarwa, 'Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source'.

135 Masarwa, 'Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source'.

136 Breaking the Silence, Military Rule: Testimonies of Soldiers from the Civil Administration, Gaza DCL and COGAT (Breaking the Silence, 2022), 41, https://www.breakingthesilence.org.il/inside/wp-content/uploads/2022/07/Military_rule_testimony_booklet.pdf.

137 Abraham, '"Order from Amazon": How Tech Giants Are Storing Mass Data for Israel's War'.

138 Abraham, '"Order from Amazon": How Tech Giants Are Storing Mass Data for Israel's War'.

139 Jennifer Cobbe et al., 'Understanding Accountability in Algorithmic Supply Chains', 2023 ACM Conference on Fairness Accountability and Transparency, 12 June 2023, 1188, https://doi.org/10.1145/3593013.3594073.

state-of-the-art AI technologies in-house."[140] This is because of significant barriers to entry, including access to "large and relevant quantities of data, potentially from multiple sources and labelled or moderated, relating to many use-cases, contexts, and subjects" as well as "scarce expertise in model training, testing and deployment, all with significant storage, compute, and networking needs."[141] As such, major companies like Microsoft and Amazon offer cloud-based AI technologies to "strategically position themselves in markets and supply chains of many kinds."[142]

Use of Amazon and Microsoft's pre-built transcription and translation functions

For the voice data stored in AWS, publicly available information does not confirm the use of its tools for transcription and translation. However, considering the abovementioned barriers to entry, it is quite possible that Unit 8200 uses Amazon Transcribe[143] and Amazon Translate[144] for the voice-surveillance data it stores on AWS.

For the data stored by Microsoft, AP News revealed that Israel uses Azure tools for the transcription and translation of "phone calls [...] and audio messages" stored in the company's cloud.[145] While the specific tools are not enumerated in leaked documents reviewed by The Guardian, their report also indicates "use by the Israeli military of Azure's "AI-powered translation and speech-to-text conversion tools,"[146] with translation accounting for "about half of the average monthly consumption."[147]

These features match the description of Microsoft's Azure Speech, which, according to its website, include speech-to-text, including the transcription of pre-recorded audio files as well as the batch transcription of large volumes of audio.[148] Other features of relevance comprise language identification, pronunciation assessment, and speech translation.[149] Given these capabilities—and the Israeli military's substantial AI consumption through Azure—there are reasonable grounds to conclude that Azure Speech services are used to process the voice data hosted in the Azure cloud.

140 Cobbe et al., 'Understanding Accountability in Algorithmic Supply Chains', 1188.

141 Cobbe et al., 'Understanding Accountability in Algorithmic Supply Chains', 1188.

142 Cobbe et al., 'Understanding Accountability in Algorithmic Supply Chains', 1189.

143 Amazon Web Services, Speech to Text Service - Amazon Transcribe, n.d., https://aws.amazon.com/pm/transcribe/.

144 Amazon Web Services, Amazon Translate, n.d., https://aws.amazon.com/translate/.

145 Biesecker et al., 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies', 18 February 2025.

146 Harry Davies and Yuval Abraham, 'Revealed: Microsoft Deepened Ties with Israeli Military to Provide Tech Support during Gaza War', The Guardian (Jerusalem), 23 January 2025, https://www.theguardian.com/world/2025/jan/23/israeli-military-gaza-war-microsoft.

147 Yuval Abraham, 'Leaked Documents Expose Deep Ties between Israeli Army and Microsoft', +972 Magazine, 23 January 2025, https://www.972mag.com/microsoft-azure-openai-israeli-army-cloud/.

148 Microsoft, What Is the Speech Service?, 5 November 2025, https://learn.microsoft.com/en-us/azure/ai-services/speech-service/overview.

149 Microsoft, What Is the Speech Service?

4.3. SPEECH ANALYTICS

While transcription and translation convert raw audio into searchable and analyzable text, the next step in Israel's voice-surveillance infrastructure likely involves the use of speech analytics, which news reporting suggests to include keyword searching and content flagging, sentiment analysis, and pattern recognition.

Keyword searching and flagging

A foundational feature of speech analytics is keyword searching. This enables the identification of relevant content within large amounts of intercepted data. An intelligence officer, speaking to AP News, described using Azure to quickly search for terms in transcripts of "conversations between two people within a 50-page document."[150] In addition to Azure, +972 Magazine reported that Unit 8200 uses its own smaller models to classify information and conduct "efficient keyword searches" across voice-surveillance data.[151]

Additionally, AP News also noted that Israeli military uses "to sift through vast troves of intelligence, intercepted communications and surveillance to find suspicious speech or behavior,"[152] though the exact tools used remain unspecified. This type of flagging can be done via a number of different techniques, but most likely involve automatically scanning text transcripts of voice data for pre-determined terms.

This capability has been proven to be used previously for written text messages in a system called "noisy message," also developed by Unit 8200 after 2015 and still in use today.[153] This system "collects Palestinians' text messages and assigns each of them a rating indicating their level of "danger."[154] Sources told The Guardian that said rating is based on an automated scan of all text messages between Palestinians in the West Bank in search of words deemed to be suspicious.[155]

Sentiment analysis

Sentiment analysis enables the identification of emotional states or intent within intercepted conversations. This can be conducted both on the audio itself (by analysing vocal markers such as the volume of a voice or the tightness of vocal cords) and on the transcribed text (via keyword analysis and content assessment). While not confirming which of the two approaches—if not both—is deployed, sources of The Guardian indicate that sentiment models are used to "automatically analyse intercepted phone conversations by identifying Palestinians expressing anger."[156] These capabilities may be powered by smaller language models developed by Unit 8200, alongside or in addition to Azure's cloud-based tools, deployed "on-prem,"

150 Biesecker et al., 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies', 18 February 2025.

151 Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'.

152 Biesecker et al., 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies', 18 February 2025.

153 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

154 Abraham, 'Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians'.

155 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

156 Davies and Abraham, 'Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data'.

short for 'on premise,' which means on the unit's own servers, and in this case in a segregated environment disconnected from the internet.[157]

Pattern recognition

There is some indication that Israel uses "a foundational model"[158] that aims to "take 'everything that has ever been collected' and detect 'connections and patterns which are difficult for a human to do alone.'"[159] Further details on this model are not available, but it was reported that Israeli private sector experts contributed to building it during their reserve duty.[160]

OpenAI's language model through Microsoft Azure

It was reported that Israel's military has access to OpenAI's GPT-4 model for the purposes of "analyzing billions of pieces of information, learning from past cases, and responding to spoken and written instructions."[161] Documents reviewed by +972 Magazine revealed that the Israeli military consumes substantial AI services from Azure, a quarter of that consumption being for GPT-4.[162] While a spokesperson for the company stated that "OpenAI does not have a partnership with the [Israeli military],"[163] Microsoft began offering OpenAI's models as part of its Azure suite of offerings after investing billions of dollars in the company. Indeed, as the +972 Magazine reporting revealed, beginning in August 2023, the Israeli army "acquires access through the Azure platform rather than directly from OpenAI"[164] (emphasis added). The fact that "OpenAI's commercial services can be accessed only through Azure" exemplifies a broader algorithmic supply chain trend where "AI-specific providers' services can be accessed only [...] that specific provider's cloud, rather than through a competitor.[165]

The processes and technologies outlined above enable the large-scale identification, transcription, translation, processing, and analysis of voice data. Once this information is processed, it can be leveraged for a variety of applications.

5. APPLICATIONS FOR VOICE DATA

Publicly available information indicates four primary applications for processed and analyzed voice data: (1) direct reporting to military and intelligence units; (2) integration with other databases through data fusion; (3) use as training material for a large language model; and (4) use as input into an automated target-generation system.

157 Abraham, '"Order from Amazon": How Tech Giants Are Storing Mass Data for Israel's War'.

158 Davies and Abraham, 'Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data'.

159 Davies and Abraham, 'Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data'.

160 Davies and Abraham, 'Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data'.

161 Abraham, 'Leaked Documents Expose Deep Ties between Israeli Army and Microsoft'.

162 Abraham, 'Leaked Documents Expose Deep Ties between Israeli Army and Microsoft'.

163 Abraham, 'Leaked Documents Expose Deep Ties between Israeli Army and Microsoft'.

164 Abraham, 'Leaked Documents Expose Deep Ties between Israeli Army and Microsoft'.

165 Cobbe et al., 'Understanding Accountability in Algorithmic Supply Chains', 1191.

5.1. DIRECT REPORTING

A core application of processed voice data is the direct dissemination of translated transcripts to operational units. As reported by Middle East Eye in 2021, transcribed "texts are translated and sent to the army's intelligence units and to Shin Bet."[166] More recent reporting corroborates this workflow: commanders "can access raw intelligence translated into Hebrew."[167] In practice, this means that intercepted voice conversations—once transcribed and translated—provide raw intelligence distributed to Israeli military and internal security agencies.

5.2. DATA FUSION

Public information about how voice-surveillance data is integrated with other data remains limited, but available sources indicate that it forms part of a broader set of databases. Yossi Sariel, former head of Unit 8200 and chief architect of its AI strategy, supposedly "led a large-scale, well-funded project that dramatically expanded Israel's surveillance of Palestinians and integrated multiple intelligence databases."[168] While the exact databases with which voice data is integrated are not specified, Sariel's writings suggest cross-referencing of "visual information, cellular data, social media connections, pictures, cellphone contacts," and potentially more,[169] echoing Elia Zureik's characterization of Israel's layers of mass surveillance data collection.[170]

Examples of such data fusion appear in recent reporting. AP News mentioned that information gathered through mass surveillance "can then be cross-checked with Israel's in-house targeting systems and vice versa."[171] Azure-based tools reportedly "find people giving directions to one another," which can be cross-referenced with military geolocation systems to pinpoint specific locations.[172] This integration of voice data with geolocation may shed light on an unnamed AI audio tool deployed by the Israeli military in Gaza to locate resistance leaders, giving an approximate location for where they were making phone calls.[173]

166 Masarwa, 'Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source'.

167 Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'.

168 Abraham, 'Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians'.

169 Harry Davies and Bethan McKernan, 'Top Israeli Spy Chief Exposes His True Identity in Online Security Lapse', The Guardian, 5 April 2024, https://www.theguardian.com/world/2024/apr/05/top-israeli-spy-chief-exposes-his-true-identity-in-online-security-lapse.

170 Zureik, 'Colonialism, Surveillance, and Population Control', 12–13.

171 Biesecker et al., 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies', 18 February 2025.

172 Biesecker et al., 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies', 18 February 2025.

173 Sheera Frenkel and Natan Odenheimer, 'Israel's A.I. Experiments in Gaza War Raise Ethical Concerns', The New York Times, 25 April 2025, https://www.nytimes.com/2025/04/25/technology/israel-gaza-ai.html.

5.3. TRAINING DATA FOR LARGE LANGUAGE MODEL

Voice-surveillance data is also used as training material for a large language model (LLM) being developed by Unit 8200. An investigation by The Guardian revealed that the unit is building an LLM specifically to inquire about the communications it intercepts from Palestinians. The amount of training data required for such a model demonstrates the unit's "large-scale retention of the content of intercepted communications,"[174] potentially far more than the supposed retention period of about a month.[175] The project of building this LLM is supported by "The Studio," linking Unit 8200 with private-sector experts from companies such as Meta, Google, Microsoft, and other firms,[176] whose assistance was specifically sought by the unit.[177]

According to Ori Goshen, co-CEO of Israeli company AI21 Labs which specializes in language models and, too, aided Unit 8200, LLMs are advantageous due to "their ability to retrieve data scattered across multiple sources. Rather than using 'primitive search tools,' officers could simply 'ask questions and get answers' from a chatbot."[178] The conversational chatbot could be queried, for example, about "whether two people had ever met."[179] Reporting suggests that while the development of this LLM began prior to October 2023,[180] it accelerated in late 2024 with additional private sector support. It remains unclear whether the model has already been deployed.[181]

The rationale for using voice-surveillance data for this LLM as opposed to an existing model is straightforward. Spoken Palestinian Arabic—whether from transcripts of calls or WhatsApp conversations—is scarcely available online, especially "in the quantity needed to train such a model."[182] Existing commercial or open-source Arabic models are trained predominantly on standard written Arabic, not the spoken dialects used by Palestinians on a day-to-day basis. Unit 8200 therefore collected "all the [spoken Arabic] text the unit has ever had" and consolidated it in a central repository to be used as a training dataset.[183]

Sources told The Guardian that this dataset ultimately comprised roughly 100 billion words, covering Palestinian and Lebanese dialects. So even when intercepted conversations had no value for strictly military intelligence purposes, they were still valuable to Unit 8200 for the training and accuracy of their model.

174 Davies and Abraham, 'Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data'.
175 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.
176 The Times of Israel, 'Israel Using AI to Pinpoint Hamas Leaders, Find Hostages in Gaza Tunnels — Report'.
177 Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'.
178 Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'.
179 Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'.
180 Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'.
181 Davies and Abraham, 'Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data'.
182 Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'.
183 Davies and Abraham, 'Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data'.

A separate chatbot to Unit 8200's LLM was announced by Shin Bet in 2023, and intended to be established on the agency's own servers.[184] However, it is unknown whether this chatbot relied on voice-surveillance data as training data.

5.4. INPUT DATA FOR MILITARY TARGET GENERATION ALGORITHM

Finally, voice data is reportedly used as one input—alongside other data sources—into automated target-generation systems, most prominently the one known as Lavender.[185] Lavender assigns individuals in Gaza a numerical "risk score," the threshold above which designates them as a human target.[186] But, as Human Rights Watch cautions, without access to Lavender it is impossible to fully determine which data points contribute to these scores.[187]

Nevertheless, there are multiple news reports indicating that voice-surveillance data feeds into target-generation algorithms like Lavender. According to +972 Magazine, three intelligence sources stated that Unit 8200's cloud-based intelligence corpus—containing voice data—has been used over the past two years to plan lethal airstrikes in Gaza.[188] The Guardian further exposed that the "enormous repositories of phone calls" stored in Azure were used to identify bombing targets.[189]

In line with their writings on the quotidian violence of Israeli surveillance, Shalhoub-Kevorkian and Otman articulate how systems like Lavender "dehumanize and marginalize the surveilled," reducing human beings to risk assessment scores rather than recognizing their humanity.[190] Through this lens, voice data becomes one more datapoint used to algorithmically classify, rate, and select human targets.[191]

6. LIMITATIONS OF ALGORITHMIC VOICE TECHNIQUES

Israel's voice-surveillance apparatus combines components—speech-to-text tools, AI-powered translation, voice recognition, and large language models—that are prone to errors and inaccuracies that can lead to the mis-identification of people and the misinterpretation of speech. Their technical

184 Yuval Mann and Korin Elbaz-Alush, 'Shin Bet Develops ChatGPT-like Tool for Detecting Threats, Chief Ronen Bar Says', YNet, 27 June 2023, https://www.ynetnews.com/business/article/hjmohud002.

185 Yuval Abraham, 'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza, 3 April 2024, https://www.972mag.com/lavender-ai-israeli-army-gaza/.

186 Human Rights Watch, Questions and Answers: Israeli Military's Use of Digital Tools in Gaza, 10 September 2024, https://www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-digital-tools-gaza.

187 Human Rights Watch, Questions and Answers: Israeli Military's Use of Digital Tools in Gaza.

188 Abraham, 'Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians'.f

189 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

190 Shalhoub-Kevorkian and Otman, 'Secrecy as Colonial Violence: The Case of Occupied East Jerusalem', 191.

191 Sarah Fathallah, 'Artificial Intelligence and the Orchestration of Palestinian Life and Death', Tech Policy Press, 12 August 2025, https://www.techpolicy.press/artificial-intelligence-and-the-orchestration-of-palestinian-life-and-death/.

failures carry real-world consequences, including wrongful arrests and lethal targeting.

AI-driven transcription and translation tools often misinterpret words or context. For example, one reported error in Israel's voice-surveillance system involved the Arabic term for "payment" being mistranslated as a "the grip on the launch tube for a rocket-propelled grenade," nearly placing individuals on target lists erroneously.[192] The chatbot developed by Unit 8200 too "had difficulty identifying modern slang and words transliterated from English."[193] This is far from an anomaly, as automatic speech recognition in Arabic demonstrates subpar accuracy rates.[194] Dialectal and pronunciation variations introduce additional complications[195] and aggravate misinterpretations, as shown by a case where a Palestinian refugee was incorrectly classified as Syrian based on his pronunciation of a single syllable.[196] These errors persist even when human review is supposedly involved. Arabic-speaking officers may catch some mistakes,[197] but confirmation bias[198] and added work[199] mean errors can go uncorrected, or commanders may want to bypass military language centers and linguistic experts entirely.[200]

Beyond translation, 'hallucinations'—algorithmic model outputs that are generated without basis in the source material—pose further risks. If in use by Unit 8200, OpenAI's translation model Whisper and other transcription tools are known to fabricate text, including "adding racial commentary and violent rhetoric."[201] Sources admit that "blind reliance on these tools" is possible,[202] raising the risk that decisions are influenced by information that never actually existed.

Furthermore, voiceprinting technologies have high false-positive rates,[203] and sentiment analysis that entails emotion recognition from one's speech

192 Biesecker et al., 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies', 18 February 2025.

193 The Times of Israel, 'Israel Using AI to Pinpoint Hamas Leaders, Find Hostages in Gaza Tunnels — Report'.

194 Fawaz S. Al-Anzi and Dia AbuZeina, 'Synopsis on Arabic Speech Recognition', Ain Shams Engineering Journal 13, no. 2 (2022): 101534, https://doi.org/10.1016/j.asej.2021.06.020.

195 Daniel Leix Palumbo and Robert Prey, 'Sounding out Voice Biometrics: Comparing and Contrasting How the State and the Private Sector Determine Identity through Voice', Big Data & Society 11, no. 4 (2024): 20539517241297889, https://doi.org/10.1177/20539517241297889.

196 Karin Bijsterveld and Anna Kvicalova, 'Forensic Voices: Cultures of Sonic Detection and Identification in the West', Sound Studies 9, no. 2 (2023): 156, https://doi.org/10.1080/20551940.2023.2232211.

197 Biesecker et al., 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies', 18 February 2025.

198 Michael Biesecker et al., 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies', AP News, 18 February 2025, https://apnews.com/article/israel-palestinians-ai-technology-737bc17af7b03e98c29cec4e15d0f108.

199 Biesecker et al., 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies', 18 February 2025.

200 Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'.

201 Biesecker et al., 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies', 18 February 2025.

202 Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'.

203 Jay Stanley, 'On the Creation of Giant Voiceprint Databases', ACLU, 16 October 2014, https://www.aclu.org/news/privacy-technology/creation-giant-voiceprint-databases.

is widely decried as unreliable,[204] reflecting both the technical limitations and the dangers of misapplied biometric identification and emotion inference.

These limitations are exacerbated by the fact that some of these tools operate as 'black boxes,' with limited visibility into how algorithmic systems generate outputs or make recommendations, blocking the possibility of tracing how conclusions are reached or correcting mistakes. However, reducing error rates may not be of concern to Israel at all: Israeli sources stated that "the most pressing issue is not necessarily the accuracy of these models, but rather the vast scope of arrests they enable." For them, the most important objective was to continuously grow the list of "suspects,"[205] regardless of accuracy.

7. IMPACTS ON PALESTINIANS

Israeli voice surveillance has profound effects on Palestinians, shaping daily life through incrimination, criminalization, and deadly consequences. These impacts remain inseparable from the broader militarized and carceral context of the occupation.

Incrimination and arrests

Voice-surveillance data directly facilitates the arrests of Palestinians. The increased scope of surveillance enabled by Unit 8200's large-scale voice datasets have allowed commanders to compile expansive suspect lists across Palestinian localities, expressly contributing to a greater number of arrests.[206] The number and frequency of arrests can be arbitrarily pre-determined, and sometimes, "it's just a division commander who wants 100 arrests per month in his area," as one source disclosed.[207] The low threshold for suspicion—often vague or unsubstantiated—enables authorities to justify detention, blackmail, or even targeted killings retroactively, using voice data to legitimize their decisions. As one source told The Guardian, "[w]hen they need to arrest someone and there isn't a good enough reason to do so, that's where they find the excuse," referring to the voice-surveillance data stored in the cloud.[208] The development of Unit 8200's large language model is predicted to accelerate the incrimination and arrest of Palestinians, worsening existing "figures showing that nearly 50 per cent of adult Palestinians in the occupied territories have been arrested at one time oranother."[209]

Chilling and criminalization of speech

The pervasive monitoring of Palestinians' conversations creates a climate of fear and self-censorship.[210] "Aware that what they say [...] may be observed

204 Jade McClain, 'Alexa, Am I Happy? How AI Emotion Recognition Falls Short', New York University, 18 December 2023, https://www.nyu.edu/about/news-publications/news/2023/december/alexa--am-i-happy--how-ai-emotion-recognition-falls-short.html.

205 Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'.

206 Davies and Abraham, 'Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data'.

207 Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'.

208 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

209 Zureik, Israel's Colonial Project in Palestine, 163.

210 Zureik, 'Colonialism, Surveillance, and Population Control', 16.

constantly,"[211] Palestinians refrain from political expression or avoid speaking as freely as they might want to,[212] anticipating that their conversations could serve as incriminating or incitement material.[213] The sweeping incitement laws put in place by Israel made way for incitement to become a common charge and intimidate Palestinians into silence,[214] including and especially humanrightsdefenders.[215]

This chilling effect takes on particularly urgent dimensions in contexts where communications can mean access to life-or-death information. As one Gaza hospital administrator explained, the constant awareness of being watched «twisted and narrowed his world» to the point where he «avoids calling his brother ‹lest he ask whether any rockets were fired from the area or whether the Israelis had arrived in the area,' and those words be misread or distorted by unseen listeners.»[216] Voice surveillance thus not only chills political expression, but prevents Palestinians from seeking life-saving information about military movements, safety conditions, or humanitarian access.

Killings and assassinations

Voice surveillance can also be directly tied to lethal outcomes. If voice-surveillance data is indeed being used as input in the Israeli military's automated target-generation systems, those consequences are even more catastrophic.[217] One tragic example reported by the Los Angeles Times is the case of Jumana, a mother who was killed in an Israeli airstrike along with her 4-day-old twins in Gaza, and whose family and colleagues suspected was wrongly targeted using AI and phone data. A friend of the family said: "There's just no justification. None," adding that "[t]he Israelis have all this technology. They target with artificial intelligence, they strike based on voiceprint, on phone signals. Couldn't they verify? Why did they attack this family?"[218]

Together, incrimination, chilling of speech, and lethal targeting illustrate the grave dangers and consequences of voice surveillance for Palestinians, making it all the more urgent and critical to contest and resist this apparatus.

211 Zureik, 'Colonialism, Surveillance, and Population Control', 17.

212 Usaid Siddiqui, '"Chilling Effect": Israel's Ongoing Surveillance of Palestinians', Al Jazeera, 8 May 2023, https://www.aljazeera.com/news/2023/5/7/chilling-effect-israels-ongoing-surveillance-of-palestinians.

213 Sophia Goodfriend, 'When Palestinian Political Speech Is "Incitement"', Jewish Currents, 15 September 2021, https://jewishcurrents.org/when-palestinian-political-speech-is-incitement.

214 Goodfriend, The Expansion of Digital Surveillance in Jerusalem and Impact on Palestinians Rights, 9.

215 Human Rights Watch, Spyware Used to Hack Palestinian Rights Defenders.

216 Mhawish, 'Watched, Tracked, and Targeted'.

217 Sarah Fathallah, 'Algorithmic Death-World: Artificial Intelligence and the Case of Palestine', Public Humanities 2 (2026): e7, https://doi.org/10.1017/pub.2025.10113.

218 Nabih Bulos, 'He Went to Register the Birth of His Twins. He Returned to Find Them Killed in an Israeli Strike', Los Angeles Times, 14 August 2024, https://www.latimes.com/world-nation/story/2024-08-14/four-day-old-twins-israeli-airstrike.

8. POTENTIAL AVENUES FOR CONTESTATION

Various actors are entangled in the voice surveillance of Palestinians, complicating accountability for its impacts on Palestinians, but also creating multiple potential avenues for contestation. These leverage points also emerge because the voice-surveillance ecosystem can be challenged by a number of actors—employees, investors, foreign governments, civil society organizations, and investigative journalists.

8.1. FRAGMENTED ACCOUNTABILITY

When looking at the voice-surveillance architecture as a whole, many actors appear to operate in concert with one another. Core players in the voice-surveillance supply chain include Israeli military and government units (such as Unit 8200 and Shin Bet), Israeli private tech firms (such as AI21 Labs and NSO), and cloud providers (such as Microsoft and Amazon). Helga Tawil-Souri discusses the importance of understanding relations of power in digital infrastructures, as, in her opinion, tracing "digital surveillance routes" allows one to realize how "Israel would emerge in spaces where it would control, own and manage [those] nodes."[219]

Data-driven supply chains are supply chains where "the flow of data between actors links them together, [and] where several actors contribute towards the production, deployment, use, and functionality of AI technologies."[220] What emerges from these orchestrations is what is known by technologists as 'the problem of the many hands.'[221] This problem stems from the fact that no one actor working in isolation is responsible for outcomes that a group of multiple actors contribute towards in different ways. As such, responsibility for these systems is distributed across a complex ecosystem of actors, making it difficult "to pinpoint precisely where responsibility for human rights violations lies,"[222] and thus creating significant fragmenting accountability.

Secrecy and evasion further compound the challenge of fully comprehending the actors and the roles they play in the voice-surveillance supply chain.[223] Israel's military units frequently decline to comment on their affairs, while foreign tech companies, including Microsoft, have publicly claimed ignorance of how their platforms were used—even when employees of local subsidiaries indicate otherwise.[224] Additionally, whereas some Israeli firms forming part of this apparatus are known, as is the case for NSO and AI21 Labs, it is quite possible—if not likely—that more companies are involved. For instance, Israeli tech firm Comm-IT supported the Israeli

219 Tawil-Souri, 'Israel's Telecommunications Lines and Digital Surveillance Routes', 208.

220 Cobbe et al., 'Understanding Accountability in Algorithmic Supply Chains', 1186.

221 Helen Nissenbaum, 'Accountability in a Computerized Society', Science and Engineering Ethics 2, no. 1 (1996): 25–42, https://doi.org/10.1007/BF02639315.

222 Amnesty International, Algorithmic Accountability Toolkit (2025), https://www.amnesty.org/en/latest/research/2025/12/algorithmic-accountability-toolkit/.

223 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

224 Davies and Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

military with migrating its data into the cloud platforms after Google and Amazon established their data centers in Israel, but it's unclear if its role relates to migrating voice-surveillance data specifically.[225] Other forms of voice surveillance have also been reportedly developed by Israeli private firms, including Toka, a company behind a tool that eavesdrops on drivers through their car's microphone, but it is not clear if it is being deployed on Palestinians.[226] In other words, there are probably other actors in the Israeli private tech sector that could be a part of this voice-surveillance architecture, though not all known to the public.

Nevertheless, even though many actors form part of this data-driven supply chain, it is crucial to recognize that their arrangements are asymmetric. Some actors, especially the Israeli military and cloud service providers, hold more relative systemic importance, while others may complete more peripheral tasks. Unit 8200—and the Israeli military writ large—occupies a central position as the entity that builds in-house voice analysis tools and models, enlists the support of other actors, acquires their technologies, as well as shares or obtains voice data with and from them. But experts also acknowledge that "major cloud providers who often control underlying technologies [hold] important positions across supply chains in many sectors."[227] Ultimately, these "asymmetries of interdependence produce asymmetries in power,"[228] where major actors are systemically more important in bearing the responsibility for a supply chain's outcomes.[229] Big Tech companies like the direct providers previously mentioned in this report as well as those investing in, acquiring, or otherwise supporting the Israeli firms involved in Israel's voice-surveillance architecture—for example, Nvidia, who is in talks to acquire AI21 Labs[230]—have de facto more power in the supply chain. When condemning the life-and-death impact of this voice-surveillance supply chain, it is important to keep in mind who has more relative responsibility and power.

8.2. ACTORS WITH POTENTIAL LEVERAGE

Employees and corporate insiders

Employees within technology companies may hold some degree of influence over whether their employers' technologies are developed, maintained, and sold. Employee-led activism has proven pivotal in Microsoft's case. The worker-led campaign group No Azure for Apartheid organized a series of protests at the company's U.S. headquarters and offices, demanding an end to contracts supporting the Israeli military.[231] Employees' knowledge of internal operations also comes into play when whistleblowers and internal sources share insider information to journalists for further public knowledge

225 Abraham, '"Order from Amazon": How Tech Giants Are Storing Mass Data for Israel's War'.

226 'Israeli Firms Turn Connected Cars into Surveillance Tools – Israeli Media', The Palestine Chronicle, 18 February 2026, https://www.palestinechronicle.com/israeli-firms-turn-connected-cars-into-surveillance-tools-haaretz-investigation/.

227 Cobbe et al., 'Understanding Accountability in Algorithmic Supply Chains', 1187.

228 Cobbe et al., 'Understanding Accountability in Algorithmic Supply Chains', 1190.

229 Cobbe et al., 'Understanding Accountability in Algorithmic Supply Chains', 1192.

230 'Nvidia in Advanced Talks to Buy Israel's AI21 Labs for up to $3 Billion, Report Says', Reuters, 30 December 2025, https://www.reuters.com/business/nvidia-advanced-talks-buy-israels-ai21-labs-up-3-billion-report-says-2025-12-30/.

231 Davies and Abraham, 'Microsoft Blocks Israel's Use of Its Technology in Mass Surveillance of Palestinians'.

and scrutiny, for instance disclosing how Unit 8200 used Azure services to storevoice-surveillancedata.[232]

Investors and shareholders

Investors wield financial and governance leverage in the companies whose shares they hold, often through formal proposals or direct engagement with corporate leadership. In July 2025, at least 60 Microsoft investors—collectively representing over $80 million in shares—filed a proposal requesting a comprehensive assessment of the company's human rights due diligence processes, "in the face of serious allegations of complicity in genocide and other international crimes.""[233] Specifically, investors requested that Microsoft assess how its AI and cloud technologies are being misused by military clients "to commit human rights abuses or violations of international humanitarian law,"[234] after investigations revealed the company's role in storing troves of Palestinian voice-surveillance data.

In December 2025, Norway's $2.1 trillion sovereign wealth fund—the world's largest and a major Microsoft shareholder—announced that it would support a shareholder vote requiring Microsoft to report on human rights risks in countries with significant concerns. Though not explicitly naming Israel, the proposal demanded transparency regarding how Microsoft identifies human rights dangers posed by its products and evaluates whether its internal controls effectively prevent abuses.[235] A few days later at Microsoft's annual shareholder meeting, these human rights proposals gained significant traction, securing support from more than a quarter of voting shares.[236]

Civil society organizations and activists

NGOs, advocacy groups, and grassroots activists provide critical public oversight. Their strategies include campaigns, petitions, protests, and media engagement. For example, an activist group, Geef Tegengas (Push Back), staged demonstrations on the rooftops of Microsoft data centers in the Netherlands, urging employees to withhold their labor and "lay down their work until all Israeli intelligence has been removed from the servers,"237 in response to news that Unit 8200 was using Azure's cloud platform, notably the data centers in the Netherlands, to store intercepted Palestinian voice data.

232 Abraham, 'Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians'.

233 Abraham, 'Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians'.

234 Layne Mullett, 'Unprecedented Investor Action Demands Microsoft Answer for Reported Involvement in Gaza Genocide', American Friends Service Committee, 23 July 2025, https://afsc.org/newsroom/unprecedented-investor-action-demands-microsoft-answer-reported-involvement-gaza-genocide.

235 Mike Ludwig, 'Microsoft Faces Reckoning for Assisting Israel's Genocide in Gaza', Truthout, 3 December 2025, https://truthout.org/articles/microsoft-faces-reckoning-for-assisting-israels-genocide-in-gaza/.

236 Todd Bishop, 'Filing: Human Rights Proposals Win More than 25% of Votes at Microsoft Shareholder Meeting', GeekWire, 9 December 2025, https://www.geekwire.com/2025/filing-human-rights-proposals-win-more-than-25-of-votes-at-microsoft-shareholder-meeting/.

237 Harry Davies, 'Activists in Netherlands Protest on Roof of Microsoft Site Storing Israeli Military Data', The Guardian, 10 August 2025, https://www.theguardian.com/world/2025/aug/10/activists-in-netherlands-protest-on-roof-of-microsoft-site-storing-israeli-military-data.

Investigative journalists

Independent investigative journalism plays a significant role in revealing abuses. Microsoft only conducted investigations—the first in May 2025[238] and the second in September of the same year[239]—into its relationship with Unit 8200 and the harm it causes to Palestinians after The Guardian, +972 Magazine, and other outlets published reports detailing how Azure was used to store and process Palestinian voice data. Investigative journalism not only triggers corporate responses but also informs the public. In fact, much of the information that this report presents on the voice-surveillance architecture deployed by Israel relies on journalistic exposés.

Foreign governments and international bodies

National governments and international bodies have the potential to apply leverage to actors in the voice-surveillance apparatus through trade policy, sanctions, or legal actions. European states, for example, debated measures to prevent the use of EU data centers for hosting voice-surveillance data, while the UN Special Rapporteur has raised the potential for corporate complicity in international crimes, which could be grounds for investigations and prosecutions by the International Criminal Court and national judiciaries.[240]

8.3. DEMANDS AND POTENTIAL COURSES OF ACTION

Suspension or cancellation of contracts

Direct demands often involve the suspension or termination of contracts, in this case those that underlie Israel's voice-surveillance architecture. In an "extraordinary decision," Microsoft ultimately "ceased and disabled a set of services to a unit within the Israel ministry of defense", including cloud storage and AI services, following combined pressure from employees, investors, and investigative reports.[241] This decision set a new precedent, as this "termination is the first known case of a US technology company withdrawing services provided to the Israeli military" since October 2023.[242] However, for some, this was only the first step of many. On the same day of the announcement, No Azure For Apartheid called for Microsoft to cut all its ties with Israel.[243] And shortly thereafter, a group of human rights groups also demanded more from Microsoft, asking its CEO "[w]hat steps, if any, will [the company] take to suspend its business with the Israeli military and other government bodies where there is evidence indicating that business is contributing to grave human rights abuses and international crimes,"[244] demanding further accountability and action.

238 Microsoft, 'Microsoft Statement on the Issues Relating to Technology Services in Israel and Gaza', Microsoft On the Issues, 15 August 2025, https://blogs.microsoft.com/on-the-issues/2025/05/15/statement-technology-israel-gaza/.

239 Brad Smith, 'Update on Ongoing Microsoft Review', Microsoft On the Issues, 25 September 2025, https://blogs.microsoft.com/on-the-issues/2025/09/25/update-on-ongoing-microsoft-review/.

240 The Office of the High Commissioner for Human Rights, From Economy of Occupation to Economy of Genocide: Report of the Special Rapporteur on the Situation of Human Rights in the Palestinian Territories Occupied since 1967, A/HRC/59/23 (2025), https://www.ohchr.org/en/documents/country-reports/ahrc5923-economy-occupation-economy-genocide-report-special-rapporteur.

241 Davies and Abraham, 'Microsoft Blocks Israel's Use of Its Technology in Mass Surveillance of Palestinians'.

242 Davies and Abraham, 'Microsoft Blocks Israel's Use of Its Technology in Mass Surveillance of Palestinians'.

243 No Azure For Apartheid, The First Domino Has Fallen — Microsoft Cuts Some Services to Israeli Unit 8200, 25 September 2025, https://medium.com/@noazureforapartheid/the-first-domino-has-fallen-microsoft-cuts-some-services-to-israeli-unit-8200-b502d63e8b3b.

244 Access Now et al., Microsoft Must Come Clean on Its Role in Israel's War on Gaza, 10 October 2025, https://www.accessnow.org/press-release/microsoft-must-come-clean-on-its-role-in-israels-war-on-gaza/.

Legal liability

Even though lawsuits have not yielded much material impact in the past, Zureik made a case for cause lawyering, thanks to "mounting interest in the potential of human rights and transnationalism to affect state policies and mobilise refugee communities." To him, cause lawyering "has proven effective in publicising mistreatment of marginal groups who have no recourse to redressing their grievances through the apparatuses of the nation-state."[245]

Companies hosting voice-surveillance data abroad may be exposed to legal liability under the legal corpus of their corresponding jurisdictions, requiring companies to comply with specific conditions to ensure human rights due diligence and abide by data protection and privacy legal provisions. This point was raised in an internal legal opinion from the Israeli Justice Ministry in 2022, which "noted that both France and Germany required corporations to check for human rights violations in their supply chains by law," adding that if "it were to be revealed that these corporations are operating in the occupied Palestinian territories, such laws 'may lead to the issuance of orders to prevent or restrict services.'"[246] In relation to the voice-surveillance data stored in Azure's Netherlands-based data centers, the ministry warned that "the Netherlands was working on similar legislation," concerned that "a potential lawsuit would be particularly harmful to Israel."[247]

The Israeli Justice Ministry's concerns were not entirely unfounded. Revelations about the Israeli military's reliance on Netherlands-based data centers to store voice-surveillance data prompted parliamentary inquiries, in response to which the Dutch foreign minister proclaimed: "If there are serious indications of criminal offences in that information, legal proceedings can of course be initiated, and that is then up to the public prosecution service."[248] In Ireland, the Irish Council for Civil Liberties formally asked the Irish Data Protection Commission to investigate Microsoft for the "unlawful processing" of the voice data of Palestinians, constituting "a breach of the EU's general data protection regulation (GDPR) governing use of personal data."[249]

Concerns of facing lawsuits can be alleviated by Israel by keeping voice-surveillance data within its jurisdiction. Given that major cloud providers have established their own data centers in Israel, one source told +971 Magazine that this could lessen the fear of legal action from overseas courts.[250] This tactic is common in algorithmic supply chains, as actors use whatever "techno-legal strategy" that enables them to reduce risk, and, in the case of cross-border supply chains, make use of regulatory arbitrage.[251] Israel can also enlist the collaboration of tech companies, as contracts negotiated with the likes of Google and Amazon stipulate that they send a secret code to Israel to tip it off "when it has disclosed Israeli data to foreign courts or

245 Zureik, Israel's Colonial Project in Palestine, 47.

246 Abraham, 'Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians'.

247 Abraham, 'Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians'.

248 Davies, 'Activists in Netherlands Protest on Roof of Microsoft Site Storing Israeli Military Data'.

249 O'Carroll, 'Irish Authorities Asked to Investigate Microsoft over Alleged Unlawful Data Processing by IDF'.

250 Abraham, '"Order from Amazon": How Tech Giants Are Storing Mass Data for Israel's War'.

251 Cobbe et al., 'Understanding Accountability in Algorithmic Supply Chains', 1194–95.

investigators," as a way "to sidestep legal orders."[252] This would allow Israel to swiftly move its data, as was the case for the data it held in Azure's data centers in The Netherlands, mere days following The Guardian investigation,[253] something the Irish Council for Civil Liberties considered akin to hiding "evidence of illegal processing before investigations could commence within the EU."[254]

Being implicated in the voice-surveillance supply chain can be in breach not only of foreign domestic laws but also international law. As an international coalition of legal and advocacy rights groups—the Abolitionist Law Center, Avaaz Foundation, European Legal Support Center, SOMO, Center for Constitutional Rights, Ekō, and GLAN (Global Legal Action Network)--warned in a notice of exposure to legal liability sent to Microsoft for its involvement in grave human rights violations, including "Israel's commission of illegal, extensive, and oppressive surveillance of the Palestinian population," the company "Microsoft has exposed itself, its leadership, and its individual officers to wide-ranging criminal and civil legal liability, including in domestic courts in the United States and the European Union, and before various international bodies"[255] such as the International Criminal Court.

Countries that recognize the International Court of Justice's power may legally challenge companies operating in their juridictions if the court ultimately rules the military campaign to be a genocide.[256] International humanitarian and human rights law offers avenues for contestation, including litigation in international tribunals and transnational lawsuits, on the grounds of violating key rights as the right to privacy, freedom of expression, and access to the internet.[257] Under the Oslo Accords, violating Palestinian sovereignty over ICT infrastructure could also be argued.[258]

Sanctions and export controls

Governments could impose targeted sanctions, export controls, or blacklisting of companies enabling human rights violations like the ones resulting from Israel's voice-surveillance apparatus. One example is the U.S. government's blacklisting of spyware companies NSO Group and Candiru.[259] Governments could also impose export controls. However, this is complicated by the "dual-use" nature of technologies used in voice surveillance, which can be used for both military and non-military purposes. For instance, "U.S. export controls were originally created to regulate items with clear military inputs and use cases," but dual-use technologies that also carry commercial

252 Harry Davies and Yuval Abraham, 'Revealed: Israel Demanded Google and Amazon Use Secret "Wink" to Sidestep Legal Orders', The Guardian, 29 October 2025, https://www.theguardian.com/us-news/2025/oct/29/google-amazon-israel-contract-secret-code.

253 Davies and Abraham, 'Microsoft Blocks Israel's Use of Its Technology in Mass Surveillance of Palestinians'.

254 O'Carroll, 'Irish Authorities Asked to Investigate Microsoft over Alleged Unlawful Data Processing by IDF'.

255 Abolitionist Law Center, 'Microsoft's Aiding of Israel's Genocide Against Palestinians Exposes Company and Its Leadership to Legal Liability', Abolitionist Law Center, 2 December 2025.

256 Ryan Grim and Waqas Ahmed, 'The Israeli Military Is One of Microsoft's Top AI Customers, Leaked Documents Reveal', Drop Site, 23 January 2025, https://www.dropsitenews.com/p/microsoft-azure-israel-top-customer-ai-cloud.

257 Anan AbuShanab, Connection Interrupted: Israel's Control of the Palestinian ICT Infrastructure and Its Impact on Digital Rights (7amleh – The Arab Center for the Advancement of Social Media, 2018), 27, https://7amleh.org/wp-content/uploads/2019/01/Report_7amleh_English_final.pdf.

258 Abdullah and Bahour, ICT: The Shackled Engine of Palestine's Development.

259 Masarwa, 'Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source'.

applications "are more difficult to regulate at both the national and international levels."[260]

The fragmented accountability and asymmetrical power dynamics of Israel's voice-surveillance ecosystem's create multiple leverage points for challenging its operations, from employee activism and investor pressure to legal action and international scrutiny. While Microsoft's precedent-setting termination of services to Israeli military units demonstrates the effectiveness of coordinated contestation, demands for further accountability and more decisive action highlight that this remains only one step in a broader struggle. Ultimately, the contested nature of this surveillance architecture—revealed through investigative journalism and scrutinized through regulatory, legal, and public pressure—offers pathways to disrupt the systems enabling Israel's algorithmic voice surveillance of Palestinians.

CONCLUSION

'Captive Voices' speaks to the profound violation at the heart of Israel's mass algorithmic voice surveillance: the systematic capture of Palestinian speech as a mechanism for their oppression. The preceding chapters have shown that the voice-surveillance apparatus deployed over Palestinians is not a discrete or isolated program, but a dense, multilayered system of capture, storage, analysis, and operational use. What emerges is an architecture of control in which voice data—an intimate, ephemeral trace of everyday life—is embedded in a broader project of population control, connected to other modes of Israeli mass surveillance. This voice-surveillance architecture deeply impacts Palestinian life: constraining communication, producing fear, and facilitating incrimination, arrests, and death.

Even within this architecture of digital control, pathways for contestation emerge. The systematic voice surveillance of Palestinians reveals not only the scale of Israel's military occupation but also the pivotal role of corporations, technology companies, and cloud service providers, all of whom can be pressured through various means. Cases like Microsoft show that actors in this apparatus are not immovable: under sustained pressure from workers, investors, journalists, civil society, and governments, they can be compelled to suspend contracts, adjust practices, or confront their own complicity in human rights abuses.

Yet, contesting this voice-surveillance apparatus means also confronting the carceral and colonial logics that made such a system imaginable and implementable in the first place. Without addressing these underlying structures—including the normalization of mass surveillance and data collection, the legal exceptionalism applied to Palestinians, and the global diplomatic and market incentives that reward Israel's securitization industry—efforts at reform risk reproducing the very logics they seek to undo.

260 Hannah Kelley, 'Dual-Use Technology and U.S. Export Controls', CNAS Technology Policy Lab, 15 June 2023, https://www.cnas.org/publications/reports/dual-use-technology-and-u-s-export-controls.

The account presented here is perhaps only the tip of the iceberg of a larger and more opaque voice-surveillance regime, but it provides an initial mapping of how the voice data of Palestinians is intercepted, processed, and weaponized. Ultimately, this report serves as both a documentation and an invitation: a call for further research, broader scrutiny, and coordinated action—all interventions that must remain grounded in the broader struggle for Palestinian human rights, dignity, and self-determination.

REFERENCES

- 7amleh. Aš-Šabāb al-Filis□yniyn Wa-Lmušārka Ās-Syāsya □abra Šabakāt at-Ttawā□ul ā-L□i-jtimā□y الشباب الفلسطينيين والمشاركة السياسية عبر شبكات التواصل الاجتماعي [Palestinian Youth and Political Participation via Social Media Networks]. 7amleh – The Arab Center for the Advancement of Social Media, 2019. https://7amleh.org/wp-content/uploads/2019/10/استطلاع-حملة1-.pdf.
- 7amleh. Facial Recognition Technology and Palestinian Digital Rights. 7amleh – The Arab Center for the Advancement of Social Media, 2020. https://7amleh.org/post/facial-recognition-technology-and-palestinian-digital-rights.
- 7amleh. Gaza Telecommunications Infrastructure: Assessment to Damages and Humanitarian Impact. 7amleh – The Arab Center for the Advancement of Social Media, 2024. https://7amleh.org/post/impact-of-war-on-gaza-s-telecommunications-infrastructure-en.
- 7amleh. Intensification of Surveillance in East Jerusalem Since October 2023. 7amleh – The Arab Center for the Advancement of Social Media, 2024. https://7amleh.org/post/surveillance-and-digital-rights-violations-in-east-jerusalem-en.
- 7amleh. Netanyahu Imposes Dangerous "Big Brother" Surveillance under the Pretext of a Security Response to the Coronavirus. 23 March 2020. https://www.apc.org/en/news/7amleh-netanyahu-imposes-dangerous-big-brother-surveillance-under-pretext-security-response.
- Abdullah, Wassim F., and Sam Bahour. ICT: The Shackled Engine of Palestine's Development. Al-Shabaka, 2015. https://al-shabaka.org/briefs/ict-the-shackled-engine-of-palestines-development/?generate_pdf=view.
- Abolitionist Law Center. 'Microsoft's Aiding of Israel's Genocide Against Palestinians Exposes Company and Its Leadership to Legal Liability'. Abolitionist Law Center, 2 December 2025.
- Abraham, Yuval. 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'. +972 Magazine, 6 March 2025. https://www.972mag.com/israeli-intelligence-chatgpt-8200-surveillance-ai/.
- Abraham, Yuval. 'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza. 3 April 2024. https://www.972mag.com/lavender-ai-israeli-army-gaza/.
- Abraham, Yuval. 'Leaked Documents Expose Deep Ties between Israeli Army and Microsoft'. +972 Magazine, 23 January 2025. https://www.972mag.com/microsoft-azure-openai-israeli-army-cloud/.
- Abraham, Yuval. 'Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians'. +972 Magazine, 6 August 2025. https://www.972mag.com/microsoft-8200-intelligence-surveillance-cloud-azure/.
- Abraham, Yuval. '"Order from Amazon": How Tech Giants Are Storing Mass Data for Israel's War'. +972 Magazine, 4 August 2024. https://www.972mag.com/cloud-israeli-army-gaza-amazon-google-microsoft/.
- AbuShanab, Anan. Connection Interrupted: Israel's Control of the Palestinian ICT Infrastructure and Its Impact on Digital Rights. 7amleh – The Arab Center for the Advancement of Social Media, 2018. https://7amleh.org/wp-content/uploads/2019/01/Report_7amleh_English_final.pdf.
- Access Now, Amnesty International, Electronic Frontier Foundation, Human Rights Watch, 7amleh, and Fight for the Future. Microsoft Must Come Clean on Its Role in Israel's War on Gaza. 10 October 2025. https://www.accessnow.org/press-release/microsoft-must-come-clean-on-its-role-in-israels-war-on-gaza/.
- Al Jazeera. 'Al-Duwairi: Al-Ā□tilāl Yast□dim Ba□maï al-□ūt Wāl□īn Lit□qwb Muqātilī al-Muqāwama Bi□aza الدويري: الاحتلال يستخدم بصمة الصوت والعين لتعقّب مقاتلي المقاومة بغزة [Al-Duwairi: The Occupation Uses Voice and Eye Scans to Track Resistance Fighters in Gaza]'. Al Jazeera, 15 April 2025. https://www.aljazeera.net/news/2025/4/15/الدويري-الاحتلال-يستخدم-بصمة-الصوت.

- Al Jazeera. 'US Court Bars Israeli Spyware Firm from Targeting WhatsApp Users'. Al Jazeera, 18 October 2025. https://www.aljazeera.com/news/2025/10/18/us-court-bars-israeli-spyware-firm-from-targeting-whatsapp-users.
- Al Jazeera. 'What Is Project Nimbus, and Why Are Google Workers Protesting Israel Deal?' Al Jazeera, 23 April 2024. https://www.aljazeera.com/news/2024/4/23/what-is-project-nimbus-and-why-are-google-workers-protesting-israel-deal.
- Al-Anzi, Fawaz S., and Dia AbuZeina. 'Synopsis on Arabic Speech Recognition'. Ain Shams Engineering Journal 13, no. 2 (2022): 101534. https://doi.org/10.1016/j.asej.2021.06.020.
- Ali, Rabia. 'Is WhatsApp Putting Palestinians at Risk of Being Killed in Gaza?' Anadolu, 30 April 2024. https://www.aa.com.tr/en/artificial-intelligence/is-whatsapp-putting-palestinians-at-risk-of-being-killed-in-gaza/3206563.
- Al-Jaafari, Wajdi. '"Mas□ūlūn: jamy' wasā'il al'itti□āl fī falas□īn murāqaba" مسؤولون: جميع وسائل الاتصال في فلسطين مراقبة [Officials: All means of communication in Palestine are monitored]'. Ma'an News Agency, 20 December 2014. https://www.maannews.net/news/748592.html.
- Alshurafa, Mohammed. The Impact of the Gaza Blockade and the Destruction of Telecommunications Infrastructure on the Digital Economy Amidst Genocide. 7amleh – The Arab Center for the Advancement of Social Media, 2025. https://7amleh.org/post/gaza-digital-economy-collapse-en.
- Amazon Web Services. Amazon Translate. n.d. https://aws.amazon.com/translate/.
- Amazon Web Services. Speech to Text Service - Amazon Transcribe. n.d. https://aws.amazon.com/pm/transcribe/.
- Amnesty International. Algorithmic Accountability Toolkit. 2025. https://www.amnesty.org/en/latest/research/2025/12/algorithmic-accountability-toolkit/.
- Amnesty International. Amnesty International and More than 170 Organisations Call for a Ban on Biometric Surveillance. 7 June 2021. https://www.amnesty.org/en/latest/press-release/2021/06/amnesty-international-and--more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/.
- Amnesty International. Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware. 8 November 2021. https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/.
- AVG. Malware Is Still Spying on You Even When Your Mobile Is Off. 14 September 2018. https://www.avg.com/en/signal/android-spyware-that-works-when-your-phone-is-off.
- Barghuthy, Eyad, and Alison Carmel. Silenced Networks: The Chilling Effect among Palestinian Youth in Social Media. 7amleh – The Arab Center for the Advancement of Social Media, 2019. https://7amleh.org/post/silenced-net-the-chilling-effect-among-palestinian-youth-in-social-media.
- Batniji, Rajaie. 'Searching for Dignity'. The Lancet 380, no. 9840 (2012): 466–67. https://doi.org/10.1016/S0140-6736(12)61280-X.
- Biesecker, Michael, Sam Mednick, and Garance Burke. 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies'. AP News, 18 February 2025. https://apnews.com/article/israel-palestinians-ai-technology-737bc17af7b03e98c29cec4e15d0f108.
- Biesecker, Michael, Sam Mednick, and Garance Burke. 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies'. AP News (Tel Aviv), 18 February 2025. https://apnews.com/article/israel-palestinians-ai-technology-737bc17af7b03e98c29cec4e15d0f108.

- Biggar, Paul. Meta and Lavender. 16 April 2024. https://blog.paulbiggar.com/meta-and-lavender/.
- Bijsterveld, Karin, and Anna Kvicalova. 'Forensic Voices: Cultures of Sonic Detection and Identification in the West'. Sound Studies 9, no. 2 (2023): 155–65. https://doi.org/10.1080/20551940.2023.2232211.
- Bishop, Todd. 'Filing: Human Rights Proposals Win More than 25% of Votes at Microsoft Shareholder Meeting'. GeekWire, 9 December 2025. https://www.geekwire.com/2025/filing-human-rights-proposals-win-more-than-25-of-votes-at-microsoft-shareholder-meeting/.
- Breaking the Silence. Military Rule: Testimonies of Soldiers from the Civil Administration, Gaza DCL and COGAT. Breaking the Silence, 2022. https://www.breakingthesilence.org.il/inside/wp-content/uploads/2022/07/Military_rule_testimony_booklet.pdf.
- Bulos, Nabih. 'He Went to Register the Birth of His Twins. He Returned to Find Them Killed in an Israeli Strike'. Los Angeles Times, 14 August 2024. https://www.latimes.com/world-nation/story/2024-08-14/four-day-old-twins-israeli-airstrike.
- Cobbe, Jennifer, Michael Veale, and Jatinder Singh. 'Understanding Accountability in Algorithmic Supply Chains'. 2023 ACM Conference on Fairness Accountability and Transparency, 12 June 2023, 1186–97. https://doi.org/10.1145/3593013.3594073.
- Conley, Julia. 'Report Indicates Israel Uses WhatsApp Data in Targeted Killings of Palestinians'. Truthout, 19 May 2024. https://truthout.org/articles/report-indicates-israel-uses-whatsapp-data-in-targeted-killings-of-palestinians/.
- Davies, Harry. 'Activists in Netherlands Protest on Roof of Microsoft Site Storing Israeli Military Data'. The Guardian, 10 August 2025. https://www.theguardian.com/world/2025/aug/10/activists-in-netherlands-protest-on-roof-of-microsoft-site-storing-israeli-military-data.
- Davies, Harry, and Yuval Abraham. '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'. The Guardian, 6 August 2025. https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud.
- Davies, Harry, and Yuval Abraham. 'Microsoft Blocks Israel's Use of Its Technology in Mass Surveillance of Palestinians'. The Guardian, 25 September 2025. https://www.theguardian.com/world/2025/sep/25/microsoft-blocks-israels-use-of-its-technology-in-mass-surveillance-of-palestinians.
- Davies, Harry, and Yuval Abraham. 'Revealed: Israel Demanded Google and Amazon Use Secret "Wink" to Sidestep Legal Orders'. The Guardian, 29 October 2025. https://www.theguardian.com/us-news/2025/oct/29/google-amazon-israel-contract-secret-code.
- Davies, Harry, and Yuval Abraham. 'Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data'. The Guardian (Jerusalem), 6 March 2025. https://www.theguardian.com/world/2025/mar/06/israel-military-ai-surveillance.
- Davies, Harry, and Yuval Abraham. 'Revealed: Microsoft Deepened Ties with Israeli Military to Provide Tech Support during Gaza War'. The Guardian (Jerusalem), 23 January 2025. https://www.theguardian.com/world/2025/jan/23/israeli-military-gaza-war-microsoft.
- Davies, Harry, and Bethan McKernan. 'Top Israeli Spy Chief Exposes His True Identity in Online Security Lapse'. The Guardian, 5 April 2024. https://www.theguardian.com/world/2024/apr/05/top-israeli-spy-chief-exposes-his-true-identity-in-online-security-lapse.
- De Luce, Dan. 'Wigs, Robotic Guns and Exploding Pagers: Israel Has a Long History of Hunting down Its Enemies'. NBC News, 20 September 2024. https://www.nbcnews.com/investigations/israel-long-history-targeted-killings-enemies-rcna171888.
- Decoster, Xavier Stephane, Ilhab Jebari, Anat Lewin, and Carlo Maria Rossotto. The Telecommunication Sector in the Palestinian Territories: A Missed Opportunity for Economic Development. No. 104263. World Bank Group, 2016. http://documents.worldbank.org/curated/en/993031473856114803.
- Demopoulos, Alaina. 'Honk Honk! Can Noise Cameras Reduce "Potentially Fatal" Sound Pollution?' The Guardian (New York), 4 October 2023. https://www.theguardian.com/us-news/2023/oct/04/new-york-noise-cameras.

- Electronic Frontier Foundation. 'Gunshot Detection'. Street Level Surveillance, n.d. https://sls.eff.org/technologies/gunshot-detection.
- Euro-Med Human Rights Monitor. Israeli Telecom Companies Must Adhere to UN Principles, Stop Fully Cooperating with Security Agencies. 13 November 2022. https://euromedmonitor.org/en/article/5437/Israeli-telecom-companies-must-adhere-to-UN-principles,-stop-fully-cooperating-with-security-agencies.
- Fathallah, Sarah. 'Algorithmic Death-World: Artificial Intelligence and the Case of Palestine'. Public Humanities 2 (2026): e7. https://doi.org/10.1017/pub.2025.10113.
- Fathallah, Sarah. 'Artificial Intelligence and the Orchestration of Palestinian Life and Death'. Tech Policy Press, 12 August 2025. https://www.techpolicy.press/artificial-intelligence-and-the-orchestration-of-palestinian-life-and-death/.
- Fathallah, Sarah, and Nick Mitchell. 'Occupied Assets: Israeli Neoliberalism and the Datafication of Palestinian Life'. Disjunctions Magazine, January 2026. https://disjunctionsmag.com/articles/occupied-assets/.
- Fayyad, Usama, Gregory Piatetsky-Shapiro, and Padhraic Smyth. 'From Data Mining to Knowledge Discovery in Databases'. AI Magazine, 15 March 1996.
- Flensburg, Sofie, and Signe Sophus Lai. 'Follow the Data! A Strategy for Tracing Infrastructural Power'. Media and Communication 11, no. 2 (2023). https://doi.org/10.17645/mac.v11i2.6464.
- Frenkel, Sheera, and Natan Odenheimer. 'Israel's A.I. Experiments in Gaza War Raise Ethical Concerns'. The New York Times, 25 April 2025. https://www.nytimes.com/2025/04/25/technology/israel-gaza-ai.html.
- Front Line Defenders. OPT/Israel: Six Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware. Front Line Defenders, 2021. https://www.frontlinedefenders.org/en/statement-report/six-palestinian-human-rights-defenders-hacked-nso-groups-pegasus-spyware.
- Goodfriend, Sophia. The Expansion of Digital Surveillance in Jerusalem and Impact on Palestinians Rights. 7amleh – The Arab Center for the Advancement of Social Media, 2021. https://7amleh.org/storage/Digital%20Surveillance%20Jerusalem_7.11.pdf.
- Goodfriend, Sophia. 'When Palestinian Political Speech Is "Incitement"'. Jewish Currents, 15 September 2021. https://jewishcurrents.org/when-palestinian-political-speech-is-incitement.
- Grim, Ryan, and Waqas Ahmed. 'The Israeli Military Is One of Microsoft's Top AI Customers, Leaked Documents Reveal'. Drop Site, 23 January 2025. https://www.dropsitenews.com/p/microsoft-azure-israel-top-customer-ai-cloud.
- Halabi, Usama. 'Legal Analysis and Critique of Some Surveillance Methods Used by Israel'. In Surveillance and Control in Israel/Palestine: Population, Territory, and Power, edited by Elia Zureik, David Lyon, and Yasmeen Abu-Laban. Routledge Studies in Middle Eastern Politics 33. Routledge, 2011. https://doi.org/10.4324/9780203845967.
- Hassan, Zaha, and H. A. Hellyer. Suppressing Dissent: Shrinking Civic Space, Transnational Repression and Palestine-Israel. Oneworld Academic, 2024.
- Human Rights Watch. Questions and Answers: Israeli Military's Use of Digital Tools in Gaza. 10 September 2024. https://www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-digital-tools-gaza.
- Human Rights Watch. Spyware Used to Hack Palestinian Rights Defenders. 8 November 2021. https://www.hrw.org/news/2021/11/08/spyware-used-hack-palestinian-rights-defenders.
- IMEU. Fact Sheet: Israeli Surveillance & Restrictions on Palestinian Movement. Institute for Middle East Understanding, 2021.
- Investigate. 'Amazon.Com Inc.' The American Friends Service Committee, 7 August 2024. https://investigate.info/company/amazon.

- Investigate. 'Microsoft Corp.' The American Friends Service Committee, 29 January 2025. https://investigate.info/company/microsoft.
- James, Robin. 'Acousmatic Surveillance and Big Data'. Sounding Out!, 20 October 2014. https://soundstudiesblog.com/2014/10/20/the-acousmatic-era-of-surveillance/.
- Jamil, Yassin. '"Tafāīl Muhila an uruq Wa asālīb al-Murāqaba as-Sirrya al-Isrāīlya Lil-Hawātif al-Jawwāla Lil-Muqāwama al-Filsīnya Wal-Lubnānya" تفاصيل مذهلة عن طرق وأساليب المراقبة السرية الإسرائيلية للهواتف الجوالة للمقاومة الفلسطينية واللبنانية [Shocking Details Emerge about Israel's Covert Methods and Techniques for Monitoring the Mobile Phones of the Palestinian and Lebanese Resistance]'. Rai Alyoum, 21 June 2016. https://www.raialyoum.com/تفاصيل-مذهلة-عن-طرق-وأساليب-المراقبة/.
- Kelley, Hannah. 'Dual-Use Technology and U.S. Export Controls'. CNAS Technology Policy Lab, 15 June 2023. https://www.cnas.org/publications/reports/dual-use-technology-and-u-s-export-controls.
- Leix Palumbo, Daniel, and Robert Prey. 'Sounding out Voice Biometrics: Comparing and Contrasting How the State and the Private Sector Determine Identity through Voice'. Big Data & Society 11, no. 4 (2024): 20539517241297889. https://doi.org/10.1177/20539517241297889.
- Leufer, Daniel. 'Sonic Surveillance: Why You Don't Want AI Snooping on You'. Access Now, 23 September 2025. https://www.accessnow.org/ai-snooping/.
- Ludwig, Mike. 'Microsoft Faces Reckoning for Assisting Israel's Genocide in Gaza'. Truthout, 3 December 2025. https://truthout.org/articles/microsoft-faces-reckoning-for-assisting-israels-genocide-in-gaza/.
- Mahmoud, Khalid Walid. 'Voiceprint: From a Verification Tool to a Tracking Technology'. The Peninsula, 19 January 2025. https://thepeninsulaqatar.com/opinion/19/01/2025/voiceprint-from-a-verification-tool-to-a-tracking-technology.
- Mann, Yuval, and Korin Elbaz-Alush. 'Shin Bet Develops ChatGPT-like Tool for Detecting Threats, Chief Ronen Bar Says'. YNet, 27 June 2023. https://www.ynetnews.com/business/article/hjmohud002.
- Marciano, Avi. 'Israel's Mass Surveillance during COVID-19: A Missed Opportunity'. Surveillance & Society 19, no. 1 (2021): 85–88. https://doi.org/10.24908/ss.v19i1.14543.
- Masarwa, Lubna. 'Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source'. Middle East Eye (Jerusalem), 15 November 2021. https://www.middleeasteye.net/news/israel-can-monitor-every-telephone-call-west-bank-and-gaza-intelligence-source.
- McClain, Jade. 'Alexa, Am I Happy? How AI Emotion Recognition Falls Short'. New York University, 18 December 2023. https://www.nyu.edu/about/news-publications/news/2023/december/alexa--am-i-happy--how-ai-emotion-recognition-falls-short.html.
- Mhawish, Mohammed R. 'Watched, Tracked, and Targeted'. New York Magazine, 3 December 2025. https://nymag.com/intelligencer/article/watched-tracked-targeted-israel-surveillance-gaza.html.
- Microsoft. 'Microsoft Statement on the Issues Relating to Technology Services in Israel and Gaza'. Microsoft On the Issues, 15 August 2025. https://blogs.microsoft.com/on-the-issues/2025/05/15/statement-technology-israel-gaza/.
- Microsoft. Microsoft to Launch New Cloud Data Center Region in Israel. 22 January 2020. https://news.microsoft.com/source/emea/features/microsoft-to-launch-new-cloud-datacenter-region-in-israel/.
- Microsoft. What Is the Speech Service? 5 November 2025. https://learn.microsoft.com/en-us/azure/ai-services/speech-service/overview.
- Mitnick, Josh. 'Here's How the Israeli Army Is Embracing Digital Transformation'. CIO, 8 February 2020.

- Mossad, Marco. 'Are Global Tech Giants Facilitating Israel's War on Gaza?' Al Majalla, 31 May 2024. https://en.majalla.com/node/318176/science-technology/are-global-tech-giants-facilitating-israel%E2%80%99s-war-gaza.
- Mossad, Marco. 'Voiceprint Technology: A Commercial Hit with Military Utility'. Al Majalla, 7 February 2024. https://en.majalla.com/node/310146/science-technology/voiceprint-technology-commercial-hit-military-utility.
- Mullett, Layne. 'Unprecedented Investor Action Demands Microsoft Answer for Reported Involvement in Gaza Genocide'. American Friends Service Committee, 23 July 2025. https://afsc.org/newsroom/unprecedented-investor-action-demands-microsoft-answer-reported-involvement-gaza-genocide.
- Niang, Sophie Marie. 'In Defence of What's There: Notes on Scavenging as Methodology'. Feminist Review 136, no. 1 (2024): 52–66. https://doi.org/10.1177/01417789231222606.
- Nissenbaum, Helen. 'Accountability in a Computerized Society'. Science and Engineering Ethics 2, no. 1 (1996): 25–42. https://doi.org/10.1007/BF02639315.
- No Azure For Apartheid. The First Domino Has Fallen — Microsoft Cuts Some Services to Israeli Unit 8200. 25 September 2025. https://medium.com/@noazureforapartheid/the-first-domino-has-fallen-microsoft-cuts-some-services-to-israeli-unit-8200-b502d63e8b3b.
- O'Brien, Danny, and Jillian C. York. 'A Slow Boat to Fast Data: Why Is Palestine Still Waiting for 3G?' Electronic Frontier Foundation, 11 November 2015. https://www.eff.org/deeplinks/2015/11/palestine-3g.
- O'Carroll, Lisa. 'Irish Authorities Asked to Investigate Microsoft over Alleged Unlawful Data Processing by IDF'. The Guardian, 4 December 2025. https://www.theguardian.com/technology/2025/dec/04/irish-authorities-asked-to-investigate-microsoft-over-alleged-unlawful-data-processing-by-idf.
- Oslo Accords. Annex III, Concerning Civil Affairs, Israeli Palestinian Interim Agreement on The West Bank and the Gaza Strip (Oslo II). 1995. https://www.peaceagreements.org/media/documents/ag985_56017411a3c68.pdf.
- Palestine Today. '"Kayfa tatana□at □lmu□□bar□t □l'isr□'□lya □al□ jaww□lik □ša□sy!?" كيف تتنصت المخابرات الإسرائيلية على جوالك الشخصي؟! [How does Israeli intelligence eavesdrop on your personal mobile phone?!]'. Palestine Today, 30 December 2013. https://palestinetodaytv.com/post/466/كيف-تتنصت-المخابرات-الإسرائيلية-على-جوالك-الشخصي.
- Privacy International. The Global Surveillance Industry. 2016. https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.
- Reuters. 'Israeli Defense Ministry Launches COVID-19 Voice-Test Study'. Reuters (Jerusalem), 24 March 2020. https://www.reuters.com/article/world/israeli-defense-ministry-launches-covid-19-voice-test-study-idUSKBN21B2YU/.
- Reuters. 'Nvidia in Advanced Talks to Buy Israel's AI21 Labs for up to $3 Billion, Report Says'. 30 December 2025. https://www.reuters.com/business/nvidia-advanced-talks-buy-israels-ai21-labs-up-3-billion-report-says-2025-12-30/.
- Sada Social. Sada Social Calls for Immediate Investigation into Meta's Leak of WhatsApp Users' Data to the Israeli Military. 18 May 2024. https://sada.social/post/sd-soshal-ydaao-l-thkyk-aaagl-ofory-ltsryb-myta-byanat-mstkhdmy-oatsab-l-algysh-alsrayly.
- Sa'di, Ahmad H. Thorough Surveillance: The Genesis of Israeli Policies of Population Management, Surveillance and Political Control towards the Palestinian Minority. Manchester International Relations. Manchester University Press, 2016.
- Salah, Hana. '"Alba□ma as-□aūtya" Adāt Isrā□īl Litanfī□ Syāsat "Atta□afya al-Jasadya" "البصمة الصوتية" أداة إسرائيل لتنفيذ سياسة "التصفية الجسدية" ["Voiceprints": Israel's Tool for Implementing "Elimination"]'. Al-Monitor, 4 February 2014. https://www.al-monitor.com/ar/contents/articles/originals/2014/02/gaza-israel-islamic-jihad-hamas-mobile-war.html.

- Salah, Mohamad Ateyyah, Mohamad Shalodi, and Mahmoud Skafi. 'Voiceprint Authentication System'. Palestine Polytechnic University, 2021. https://scholar.ppu.edu/bitstream/handle/123456789/7547/Voiceprint-Authentication-System.pdf.
- Shalhoub-Kevorkian, Nadera. Security Theology, Surveillance and the Politics of Fear. 1st edn. Cambridge University Press, 2015. https://doi.org/10.1017/CBO9781316159927.
- Shalhoub-Kevorkian, Nadera, and Abeer Otman. 'Secrecy as Colonial Violence: The Case of Occupied East Jerusalem'. In Decolonizing the Study of Palestine: Indigenous Perspectives and Settler Colonialism after Elia Zureik, edited by Ahmad H. Sa'di and Nur Masalha. I.B. Tauris, 2023. Secrecy as Colonial Violence.
- Siddiqui, Usaid. '"Chilling Effect": Israel's Ongoing Surveillance of Palestinians'. Al Jazeera, 8 May 2023. https://www.aljazeera.com/news/2023/5/7/chilling-effect-israels-ongoing-surveillance-of-palestinians.
- Smalley, Suzanne. 'NSO Seeks to Overturn WhatsApp Case, Saying It Is "Catastrophic" for the Spyware Maker'. The Record, 20 November 2025. https://therecord.media/nso-seeks-to-overturn-whatsapp-case.
- Smith, Brad. 'Update on Ongoing Microsoft Review'. Microsoft On the Issues, 25 September 2025. https://blogs.microsoft.com/on-the-issues/2025/09/25/update-on-ongoing-microsoft-review/.
- Stanley, Jay. 'On the Creation of Giant Voiceprint Databases'. ACLU, 16 October 2014. https://www.aclu.org/news/privacy-technology/creation-giant-voiceprint-databases.
- Swinhoe, Dan. AWS Launches Israeli Cloud Region in Tel Aviv. 2 August 2023.
- Tawil-Souri, Helga. 'Digital Occupation: Gaza's High-Tech Enclosure'. Journal of Palestine Studies 41, no. 2 (2012): 27–43. https://doi.org/10.1525/jps.2012.XLI.2.27.
- Tawil-Souri, Helga. 'Hacking Palestine: A Digital Occupation'. Al Jazeera, 9 November 2011. https://www.aljazeera.com/opinions/2011/11/9/hacking-palestine-a-digital-occupation.
- Tawil-Souri, Helga. 'Israel's Telecommunications Lines and Digital Surveillance Routes'. In Decolonizing the Study of Palestine: Indigenous Perspectives and Settler Colonialism after Elia Zureik, edited by Ahmad H. Sa'di and Nur Masalha. I.B. Tauris, 2023.
- Tawil-Souri, Helga. 'Surveillance Sublime: The Security State in Jerusalem'. Jerusalem Quarterly, no. 68 (December 2016): 56–65. https://doi.org/10.70190/jq.168.p56.
- The Office of the High Commissioner for Human Rights. From Economy of Occupation to Economy of Genocide: Report of the Special Rapporteur on the Situation of Human Rights in the Palestinian Territories Occupied since 1967. A/HRC/59/23. 2025. https://www.ohchr.org/en/documents/country-reports/ahrc5923-economy-occupation-economy-genocide-report-special-rapporteur.
- The Palestine Chronicle. 'Israeli Firms Turn Connected Cars into Surveillance Tools – Israeli Media'. 18 February 2026. https://www.palestinechronicle.com/israeli-firms-turn-connected-cars-into-surveillance-tools-haaretz-investigation/.
- The Times of Israel. 'Israel Using AI to Pinpoint Hamas Leaders, Find Hostages in Gaza Tunnels — Report'. The Times of Israel, 26 April 2025. https://www.timesofisrael.com/israel-using-ai-to-pinpoint-hamas-leaders-find-hostages-in-gaza-tunnels-report/.
- Zureik, Elia. 'Colonialism, Surveillance, and Population Control'. In Surveillance and Control in Israel/Palestine: Population, Territory, and Power, edited by Elia Zureik, David Lyon, and Yasmeen Abu-Laban. Routledge Studies in Middle Eastern Politics 33. Routledge, 2011. https://doi.org/10.4324/9780203845967.
- Zureik, Elia, and David Lyon. 'Coronavirus Surveillance and Minority Groups in Israel/Palestine'. The Middle East International Journal for Social Sciences 3, no. 3 (2021): 197–215.
- Zureik, Elia T. Israel's Colonial Project in Palestine: Brutal Pursuit. Routledge Studies on the Arab-Israeli Conflict 20. Routledge, 201

PAID NARRATIVES: **DISINFORMATION AND STATE INFLUENCE THROUGH GOOGLE ADS**

MELODY SEPAHPOUR-FARD

Abstract	110
Introduction	110
Background	112
Methods	120
Results	123
Discussion	132
Conclusion	133

Melody is a PhD candidate in Data Science at the University of Limerick. With a background in psychology and computational social science, Melody's research examines online identity, discourse, and disinformation. She has explored topics ranging from vaccine misinformation to networked activism across languages.

Melody's research project analyzes online ads targeting European audiences, particularly campaigns by the Israeli Government Advertising Agency. She studies how these ads evolve, spread misinformation, and shape public opinion, assessing compliance with corporate and EU policies and their real-world consequences.



ABSTRACT

This article examines the use of Google advertising as a tool of state-linked information influence, focusing on a seven-month-long corpus of advertisements attributed to the Israeli government. Drawing on an original dataset collected from Google's Ads Transparency Center, the study identifies recurring thematic clusters such as campaigns targeting international legal institutions, and humanitarian reporting on Gaza, that coincide with moments of heightened political and media attention. The analysis combines quantitative and qualitative methods. First, it maps the temporal dynamics, geographic targeting, and thematic distribution of adver-tisements, showing that campaign activity is organized in short, high-intensity bursts aligned with specific events. Second, it estimates advertisement exposure using impression ranges and reconstructs daily visibility patterns, revealing how a small number of themes dominate au-dience reach. Third, it conducts a qualitative analysis of an advertisement to examine how narratives are constructed, with particular attention to strategies of decontextualization, fram-ing, and delegitimization of international actors. The findings suggest that Google Ads function as a high-impact infrastructure for strategic communication, enabling state actors to insert preferred narratives at moments when users actively seek information about contested issues. While these advertisements are not classified as political under platform policies, they often address politically sensitive topics and may contribute to the dissemination of disinformation at scale. The article concludes by discussing the implications for disinformation research, platform governance, and the regulation of issue-based advertising in digital environments.

1. INTRODUCTION

A few days after the October 7th, 2023 attacks on Israel, official Israeli accounts claimed that Hamas fighters "beheaded 40 babies" [41, 40]. This story was largely spread across Western media, with then-US President Biden even claiming he saw pictures of the babies [10]. This accusation represents one of the most shocking and consequential pieces of disinformation to emerge from the reports on the event. Despite being quickly debunked by journalists and fact-checkers who found no evidence to support the claim, the story continued to circulate and shape perceptions of the conflict [10]. The persistence of this disinformation exemplifies how emotionally charged narratives, once released into the information ecosystem, develop remarkable resilience against factual corrections due to their ability to tap into deep-seated biases and beliefs [45]. These emotionally resonant images of extreme brutality against innocents babies aimed at preventing rational debate and encouraging public support for military intervention.

The "40 beheaded babies" narrative was not an isolated incident but part of a broader pattern of disinformation[1] that emerged in relation to the October 7th attacks.

Multiple other claimscirculated widely in media discourse despite lacking credible verification: Hamas using human shields as a systematic policy,

[1]False information intentionally shared to cause harm [73]

widespread sexual violence and rapes committed by Hamas fighters, Hamas intelligence operatives embedded in UNRWA, etc. These examples demonstrate a pattern where unverified or contextually distorted claims are rapidly amplified through official channels and media outlets, creating what scholars term an "echo chamber effect"[2] where repetition, emotional intensity, and the confirmation bias3 outweigh factual verification [16, 45].

Beyond merely creating negative tropes about Palestinians, Israeli disinformation campaigns strategically construct narratives that provide moral justification for war and genocide. The power of such false narratives lies not only in dehumanizing the target population but in creating a moral imperative for military action by portraying the conflict as a battle between civilization and barbarism.

Today's digital ecosystem enables instantaneous worldwide propagation of false narratives. The internet has allowed disinformation to bypass traditional gatekeepers and spread virally across social media platforms, search engines, and messaging apps. This technological era has created unprecedented conditions for manipulating public opinion in real-time, with false narratives about conflicts reaching millions within hours and shaping global perceptions before fact-checking efforts can even begin [62, 71].

Many studies have studied disinformation online [48, 15, 9, 67], both through individuals and or-ganized groups related to foreign influence [47, 43, 51]. Most of the research in the domain of foreign influence has focused on Russian influence in Western societies, detailing sophisticated campaigns that employ bot networks, troll factories, and coordinated social media manipulation to influence elections, undermine democratic institutions, and shape geopolitical narrative [11, 36, 49, 30, 46]. However, disinformation originating from other state actors such as Israel, is largely understud-ied. For instance, research conducted by the EU's East StratCom Task Force in the EUvsDisinfo project has systematically documented the strategies, narratives, and cross-border impacts of Rus-sian state-sponsored disinformation across multiple countries and political contexts [27]. In contrast, despite numerous documented instances of Israeli disinformation, systematic academic investiga-tion of Israeli state-sponsored disinformation campaigns remains notably absent from the scholarly landscape. This research gap persists despite clear evidence that Israeli authorities employ sophisti-cated information operations strategies, have access to Western media and technological platforms, and engage in systematic efforts to shape international perceptions of the Israeli-Palestinian conflict [29, 42, 4, 2, 3, 68].

[2]The formation of opinion-based groups with rare exposure to diverse perspectives on social media, reinforcing shared beliefs [16]
[3]The systematic tendency of individuals to search, interpret, remember, and give greater weight to information that confirms their pre-existing beliefs, expectations, or hypotheses [53]

This paper addresses several critical research questions:

How is Google's advertising platform used by the Israeli government as a tool of information influence?

What are the temporal, thematic, and geographic characteristics of these advertising cam-paigns?

How are narratives constructed within these advertisements, and to what extent do they rely on misleading or decontextualized representations?

To answer these questions, our study employs a mixed-methods approach that combines quan-titative analysis of Google ad data with qualitative analysis of the narratives constructed in these ads. Through quantitative methods, we will analyze the ad content, targeting strategies, dissemina-tion patterns, and reach of Israeli government disinformation campaigns across Google's platforms. Complementing this quantitative analysis, the study includes a qualitative examination of an ad-vertisement to analyze how narratives are constructed and how disinformation is produced through techniques such as selective quotation, decontextualization, and misleading framing. This dual methodology allows us to both document the mechanics of digital disinformation and uncover its ideological functions in construct-ing Palestinian identities as threats to be eliminated rather than people deserving of rights.

The following background section proceeds in three parts to examine the mechanisms of Israeli disinformation and its amplification through digital platforms. First, we establish a comprehen-sive theoretical framework for understanding disinformation, analyzing its cognitive foundations, and persistent challenges in mitigation. Second, we examine Israeli hasbara, i.e., Israel's state-orchestrated system of public diplomacy and strategic communication aimed at shaping interna-tional perceptions of Israeli policies and actions, particularly in relation to Palestine. We will trace its historical evolution, objectives, and methodologies in shaping global narratives about Israel and Palestine. Finally, we investigate Google's role as a platform benefiting from and amplifying disin-formation. Together, these three parts provide a multidimensional analysis of how disinformation is created, strategically deployed, and amplified by the Israeli government through digital platforms in the context of the genocide of the Palestinian people by Israel [7, 70], offering insights into the complex interplay between state power, digital platforms, and information manipulation from the Israeli government as an understudied actor.

2. BACKGROUND

This section provides the conceptual and empirical context for the study. It first reviews the definition and mechanisms of disinformation, then examines existing evidence on Israeli state-linked information influence, and finally discusses Google's role as an infrastructure of political visibility and advertising-based influence.

2.1 DISINFORMATION: DEFINITION AND MECHANISMS

This subsection outlines the conceptual foundations of disinformation. It first clarifies key defini-tions used in the literature, then reviews the main psychological and communicative mechanisms that explain its effectiveness, and finally situates the discussion within the broader literature, which has largely focused on Russian state influence.

2.1.1 Definition

When conducting research on "fake news" and information disorder, it is important to recognize that false content is not a single phenomenon, but a set of related practices with different motivations, production chains, and harms. In a widely used framework, Wardle and Derakhshan [73] distinguish misinformation (i.e., false information shared without intent to harm) from disinformation (i.e., false information knowingly created and shared to cause harm), and from malinformation (i.e., genuine information weaponized to cause harm). This distinction is analytically useful as it foregrounds the role of intent and harm, and it consider different possible actors involved in creation, production, and distribution of information [73].

However, the broader literature does not consistently apply these categories: several studies use "misinformation" as an umbrella term that includes deliberate political manipulation [45, 23]. In addition, influential work on "fake news" often defines the phenomenon as fabricated informa-tion that mimics news media content in form but not in organizational process or intent, placing emphasis on deception and strategic imitation rather than only factual inaccuracy [44].

This paper uses disinformation as its primary term for two reasons. First, the empirical cases motivating this study concern the strategic use of false or misleading claims in a conflict environ-ment, where the objective is plausibly to shape perceptions, legitimize violence, or delegitimize an outgroup. These reasons align more closely with intentional political communication than with accidental error and this distinction is necessary if we want to understand the reasons behind the spread of false information [73]. Second, because the project focuses on state-linked campaigns and paid dissemination infrastructures (e.g., advertising systems), the agent and its incentives are central to the analysis, which is precisely what the disinformation concept is designed to capture [73, 74].

2.1.2 Mechanisms

Emotions and Repetition

Disinformation is most persuasive when it is emotionally arousing, visually compelling, easily repeated, embedded in a coherent story, and with a powerful narrative [73, 17, 38, 58]. Research in psychology shows that people are more likely to share information that evokes strong emotions (e.g., disgust, fear, outrage), often regardless of its truth value [12, 38]. Atrocity narratives—especially those involving children—can therefore be powerful examples of this logic, because they generate immediate moral outrage and provide a vivid mental image that can outlive later corrections [20]. They have three main objectives [20]: 1) demonize the enemy, 2) mobilize domestic and interna-tional support, 3) justify escalation or intervention.

Their function is not to provide actual detail, but to create a moral schema in which one side is human and the other monstrous [20]. Repetition further increases perceived credibility. Classic work on rumor transmission found that belief in wartime rumors is strongly predicted by simple repetition [5]. Later research shows that repeated statements feel more familiar and therefore more "true", even when the repetition is shallow or incidental, a phenomenon known as the illusory truth effect [37]. In political contexts, this creates a structural risk: even well-intentioned fact-checking can inadvertently spread the false claim by increasing its familiarity [44, 23].

Cognitive Biases

Disinformation is especially effective when it confirms preexisting beliefs. The confirmation bias is the tendency to seek, interpret, and remember information in ways that confirm prior be-liefs [53]. Prior research in political communication shows that audiences prefer attitude-consistent information (selective exposure) and evaluate opinion-congruent claims as more persuasive than opinion-incongruent ones [63]. People may also accept information because it is psychologically desirable—i.e., the social desirability bias [25, 24, 44]. In relation to disinformation, these mech-anisms matter because stereotypes and racialized imaginaries can function as preconceptions that make extreme claims feel plausible [57]. When new information fits existing assumptions about a target group, it is processed more fluently and is less likely to trigger skepticism; when it violates prior beliefs, people are more likely to scrutinize it or reject it [45, 23]. In other words, disinformation does not persuade from scratch; it often succeeds by activating what audiences already assume.

Persistence and Failure of Corrections

Although corrections are frequently presented as the primary remedy to disinformation, research consistently demonstrates that their impact is limited. In many cases, the effects of disinformation persist even after corrections are received, understood, and remembered, revealing a systematic asymmetry between the power of disinformation to shape mental representations and the compar-atively weak capacity of corrective information to undo them. The synthesis by Lewandowsky, Ecker, and Cook [45] reviews evidence for the continued influence effect : even when people receive and remember a retraction, they may continue to rely on the misinformation in reasoning and memory. A meta-analysis confirms that misinformation tends to retain measurable influence after correction across many contexts [72]. The meta-analysis found that corrections are significantly less effective when the original misinformation was attributed to a credible source, when it had been repeated multiple times prior to correction, or when there is a temporal delay between exposure to the misinformation and its subsequent retraction. By contrast, corrections tend to be more successful when they are coherent, align with the audience's existing worldview, and are issued by the same source that initially conveyed the misinformation. Contemporary reviews argue that resistance to correction is shaped by both cognitive factors (intuitive thinking, memory failures, familiarity) and socio-affective factors (identity, group membership, source cues, belief system or worldview, emotions) [23]. One reason corrections can fail is that misinformation often provides a simple causal story. Retractions may create an explanatory gap unless they are paired with an alternative narrative that

restores coherence, an approach shown to improve correction effectiveness [45]. Another reason is that people may forget the context in which they encountered the claim while retaining the emotional impression and the association, particularly under conditions of high repetition [44, 37].

2.1.3 Literature Focus on Russia

Institutional and academic work on disinformation has disproportionately centered on Russian state influence, especially after the 2016 U.S. election and subsequent European concerns about informa-tion warfare [11, 36, 49, 30, 46]. A key institutional anchor is the EU East StratCom Task Force and its project EUvsDisinfo, which catalogs and analyzes recurring pro-Russian disinformation narratives and their circulation across countries [27]. This emphasis has helped define disinforma-tion in much policy and public discourse: a foreign state actor deploying coordinated messaging to destabilize political cohesion, trust, and the democratic system [54, 28]. The RAND Corporation's influential report on the "firehose of falsehood" model synthesizes lessons about modern Russian propaganda, emphasizing (1) high volume and multi-channel dissemination, (2) rapid, continuous repetition, (3) lack of commitment to objective reality, and (4) inconsistent messaging designed to confuse and overwhelm [56]. Rather than persuading through careful argumentation, this approach aims to shape the informational environment through saturation, speed, and repetition, to create familiarity and therefore the difficulty of correction [56, 37, 45].

A major channel of disinformation dissemination is through computational propaganda or cyber troops and how states organize social media manipulation as a strategic practice. The Oxford Internet Institute's global inventories show that organized social media manipulation is widespread and increasingly professionalized across many countries, not only Russia [13, 14]. Platform-facing definitions also reflect this orientation: Facebook's security team defined "infor-mation operations" as coordinated actions by governments or organized actors to distort political sentiment, often using fake accounts and coordinated amplification [74].

Together, these bodies of work support three main conclusions: (1) disinformation is often organized and strategic, not spontaneous; (2) digital infrastructures and platform affordances are central to its effectiveness; and (3) repetition, amplification, and identity-congruent narratives make disinformation unusually resilient to correction [56, 23].

2.2 DISINFORMATION FROM THE ISRAELI STATE

This subsection examines the organization and characteristics of Israeli state-linked influence op-erations. It first reviews evidence on the scope of such operations, and then discusses the concept of hasbara as a framework for understanding Israel's strategic communication practices.

2.2.1 Scope of Operations

While Israel is not usually taken as a case study in this literature, multiple streams of evidence in-dicate that Israel-linked influence activity exists and spans state, private actors, and citizens. The Oxford Internet Institute (OII)

"Cyber Troops" inventories categorize Israel as a high-capacity, permanent, centrally coordinated actor in organized social media manipulation, alongside states such as Russia, China, Saudi Arabia, and the United States [14]. High-capacity cyber troop teams are characterized by their engagement in both foreign and domestic operations, the use of coordi-nated human operators and automated accounts, and, in some cases, the allocation of resources to state-sponsored media and overt propaganda efforts [14].

OII's 2019 inventory further reports evidence of formal training, team size estimates of up to ap-proximately 400 personnel, and multiple contracts valued at 778K USD and 100M USD associated with Israel's cyber troop capacity [13]. These activities span multiple platforms, including Face-book, Twitter, and Instagram, and employ a range of strategies such as pro-government messaging, attacks on political opponents, suppression of dissenting narratives, manipulated or misleading me-dia, data-driven targeting, trolling, and coordinated amplification [13, 14]. Notably, OII documents formal coordination between government agencies and civil society or citizen groups in several coun-tries; in cases including Israel, student or youth groups have reportedly been recruited or hired by government bodies to engage in computational propaganda, blurring the boundary between state and grassroots participation [13].

Platform enforcement actions and investigative reporting provide further evidence of this hybrid ecosystem. Between 2019 and 2020, Meta (Facebook) dismantled multiple coordinated inauthentic behavior networks originating in Israel that targeted audiences across Africa, Latin America, and Southeast Asia, some of which were linked to the Israeli-based private firm Archimedes Group [31, 66]. According to Meta's investigation, the operators behind these networks relied on fake accounts to manage pages, disseminate content, and artificially inflate engagement. They routinely misrepresented themselves as local actors and posted about political news and electoral processes, illustrating a systematic effort to influence political discourse while concealing the origin and coordination of the operation [31].

2.2.2 Israel's Hasbara

To better understand the organization, persistence, and strategic logic of Israeli disinformation and information influence, it is necessary to situate these practices within the longer tradition of

Israeli public diplomacy commonly referred to as hasbara. Israeli strategic communication is often described as hasbara—a Hebrew term commonly translated as "explanation" and often rendered as public diplomacy—to describe long-standing efforts to shape international perceptions of Israel. While hasbara is typically framed by official actors as a neutral practice of "explaining Israel's position" to foreign publics, critical scholarship emphasizes its political and ideological dimensions [8, 61]. Scholars have conceptualized hasbara not as conventional public diplomacy but as a state-orchestrated communicative project aimed at managing and countering international critique of Israel, particularly in relation to Palestinian self-determination [8, 61].

In the digital era, these practices have undergone a significant transformation, giving rise to what Aouragh terms "Hasbara 2.0" [8]. This shift reflects both a technological adaptation from traditional broadcast and print media to social media and digital platforms and an intensification of Israel's public diplomacy apparatus [8]. Following critical assessments of Israel's media performance during the 2006 Lebanon war and subsequent conflicts in Gaza, Israeli state and military institu-tions increasingly treated external communication as an essential strategic domain. This led to a more coordinated and professionalized communication strategy, in which legitimacy management was explicitly integrated into military doctrine and synchronized with political, legal, and media efforts. Crucially, Hasbara 2.0's central targets are foreign publics and political elites, particularly in Western states whose diplomatic, military, and financial support is considered vital [8].

Importantly, this is not merely a historical or episodic phenomenon: Israel has significantly expanded the financial resources dedicated to these efforts. In the 2026 state budget, the Ministry of Foreign Affairs—one of the key agencies involved in external communication—was allocated approximately $729 million for public diplomacy and hasbara campaigns, more than quadruple the budget allotted for similar purposes in 2025 (around $150 million), and dramatically larger than pre-war budgets that were a small fraction of current spending levels [64]. This unprecedented financial commitment will support for example international social media campaigns, influencer partnerships, and trips for foreign elected officials and civic leaders, illustrating the scale at which such strategic communication has been institutionalized [64].

The scale and professionalization of these initiatives highlight that influence is increasingly ex-ercised not only through official channels, but also through platform-mediated infrastructures that enable paid amplification, sophisticated audience targeting, and algorithmic manipulation. These dynamics are particularly salient for the present study, which focuses on disinformation on Google, especially how strategic misinformation can circulate through Google Ads. The following subsec-tion therefore turns to Google as an actor in contemporary information environments, through its advertising and search systems

2.3 GOOGLE AS AN INFRASTRUCTURE OF POLITICAL VISIBILITY AND INFLUENCE

This subsection analyzes Google's role in shaping access to information and political visibility. It first discusses the influence of search engines, then examines the auction-based logic of Google Ads, and finally explores how search advertising can be used to disseminate misleading or contested information, including documented cases involving Israeli government campaigns.

2.3.1 Influential Role of Google and Search Engines

Google Search functions as a dominant intermediary between users and online information, shaping what is encountered, trusted, and acted upon in everyday political sense-making [50]. Survey evidence shows Google's

longstanding dominance among search users [60]. Because users tend to treat high-ranked results as more credible and relevant, ranking and visibility on search engines can structure downstream judgments and choices [55]. Experimental work further suggests that biased search rankings can shift the preferences of undecided voters, implying that search ordering can have measurable political consequences even without changing the underlying content ecosystem [26].

Google's scale amplifies these effects: Google disclosed that it now processes more than 5 trillion searches per year [35]. This matters for disinformation research because search is not merely a passive index of the web; it is a high-volume, high-trust gateway through which political narratives can be discovered, reinforced, or strategically inserted into moments of uncertainty and breaking news [50].

2.3.2 Google Ads: Auction-Based Visibility and the Attention Business Model

Figure 2: The Adtent advertisement.

Google's core revenue model remains deeply tied to advertising. Alphabet's annual reporting emphasizes that Google Services revenue is generated primarily through advertising delivered on Google Search and other properties such as YouTube [6]. In Google Search, visibility is structured through an auction system in which advertisers bid to appear for particular queries; ad placement depends not only on bids but also on platform-defined relevance and quality signals [32]. As a result, the ability to pay can translate directly into visibility at the moment a user seeks information.

This auction logic is important to our research because it provides a mechanism by which po-litical actors can purchase attention and steer interpretation even when users are searching for neutral or institutional sources (e.g., humanitarian agencies), the top of the page can be populated by sponsored messages that frame what the user is about to read [75]. Importantly, research in cognitive psychology and political communication shows that early exposure to information exerts a disproportionate influence on judgment and memory. When misleading or strategically framed content is encountered first, it can function as an anchor or mental schema for subsequent infor-mation, shaping impressions even when users later encounter corrective or contradictory material [52, 45]. This primacy effect is particularly consequential in search environments, where users often scan only the top results and may not critically distinguish between sponsored and organic content, allowing initial frames to persist implicitly and influence perceptions without conscious awareness [55, 26].

2.3.3 Misinformation and Disinformation via Google Search Advertising

In the context of the 2016 U.S. election, Metaxa and Torres-Echeverry analyze candidate-related queries and report that a substantial share of candidates had search results affected by potentially fake or biased content, underscoring the vulnerability of search-mediated knowledge environments during elections [50]. More broadly, work on the political economy of disinformation argues that digital advertising markets can incentivize or sustain misleading content by monetizing attention and channeling resources toward actors who can optimize reach [21]. Related evidence shows that advertising systems can financially sustain misinformation supply chains,

highlighting how commercial incentives intersect with information integrity [1].

Google's advertising enforcement is structured around policy categories. Under Google's misrep-resentation policy, Google may suspend advertisers if it determines that an advertiser or destination is deceptive, based on review of ads, websites, accounts, and third-party sources [33]. The policy prohibits ads that mislead users by omitting relevant information about products, services, or busi-nesses; misrepresenting affiliations with other entities; providing misleading pricing or unavailable offers; or employing deceptive designs that obscure the ad's nature or intent [33]. It also bars coordinated deceptive practices in political and social issue contexts, such as concealing an adver-tiser's origin when targeting users in other countries [33]. Violations of this policy are considered egregious and can result not only in ad disapproval but in immediate suspension of the advertiser's Google Ads account, especially when the misinformation poses material harm to users [33]. Sep-arately, Google maintains a political content policy that defines and regulates "election ads" in many jurisdictions through verification, disclaimers, and other requirements [34].

This matters analytically because a government-sponsored campaign may be politically conse-quential without falling under Google's "election ads" definitions. For example, ads attacking the credibility of a UN agency or contesting famine reporting can shape public opinion about a war and humanitarian accountability while not necessarily featuring parties, candidates or election-related advertising, and thus may be treated by the platform as standard advertising rather than regulated political advertising under Google's election-ad framework [34, 65].

2.3.4 Israeli government ads on Google Ad UNRWA Case

Investigative reporting provides a concrete illustration of how state messaging can operate through Google Search ads. In 2024, WIRED reported that Israel's Government Advertising Agency bought Google Search ads against queries for "UNRWA" and "UNRWA USA," directing users to a government webpage presenting allegations intended to undermine trust in the agency [75]. The report describes how this strategy targeted donor intent (i.e., searches by people seeking the organization) and leveraged the search page to spread disinformation for legitimacy [75]. According to figures cited in that reporting, across hundreds of UNRWA-related queries, Israel-linked ads appeared a substantial share of the time when eligible; specifically, from May through July, Israel-linked ads appeared in 44% of the instances that both they and UNRWA USA ads were eligible to show, while UNRWA USA ads appeared in only 34% of those eligible circumstances, illustrating how paid visibility can outperform a targeted organization's own sponsored messaging [75].

Complainants argued that the ads were misleading and confusingly used UNRWA-related brand-ing. Early versions of the campaign were particularly explicit: according to WIRED, Israel aired Google ads in the United States stating that "UNRWA is inseparable from Hamas" and that the agency "keeps employing terrorists," messaging that UNRWA feared could shape public

opinion at a moment when U.S. political and financial support for UNRWA was already under strain [75]. After complaints were raised initially, Google removed some of these ads; however, Israel later re-sumed the campaign using revised phrasing. Screenshots reviewed by WIRED show ads promoted under headlines such as "UNRWA Neutrality Compromised," "Israel Unveils UNRWA Issues," and "Israel Advocates for Safer, Transparent Humanitarian Practices," which softened the language while directing users to substantially similar allegations [75]. Google's position, as reported, was that the ads did not violate its policies, specifically "making claims that are demonstrably false and could significantly undermine participation or trust in an electoral or democratic process." and the use of someone else's trademarks "in a confusing, deceptive, or misleading way". This episode suggests that, in practice, contested political claims can persist in paid search inventory when they are framed as advocacy or critique rather than as verifiable factual assertions that clearly trigger misrepresentation enforcement, even when the underlying narrative remains unchanged [33, 75].

Gaza Famine Case

In 2025, The Washington Post reported on internal complaints regarding Israel's government ads on YouTube and Google that asserted "There is food in Gaza" and rejected famine reporting as media bias, with Google concluding that the ads did not violate its policies [65]. Parallel coverage described large-scale spending allocations ($ 45 millions) for such campaigns and framed them as coordinated public information dissemination efforts running through Google advertising infrastructure [69, 22].

3. METHODS

This section describes the data collection process and analytical approach used in the study. It details the construction of the dataset, the manual classification of advertisement themes, the restructuring of the data for analysis, and the methods used to estimate ad exposure. It concludes with a brief presentation of illustrative examples of advertisements.

3.1 DATA COLLECTION

This study relies on advertising data collected from the Google Ad Transparency Center. We collected all advertisements published by two advertisers, the "Israeli Government Advertising Agency" and the "Israel's Government Advertising Agency", within the European Economic Area (EEA) and Turkey. The data was collected on October 15 2025, spans the period from March 22, 2025 to October 14, 2025 and contains information on both advertisers and individual ads. The collected dataset, referred to as the creative stats table, includes:

- Advertiser-level information: legal name, disclosed name, verification status, location
- Ad-level information: impression ranges per region (including aggregate EEA impressions) first and last shown dates, ad format (e.g., video, image), platform-provided topic classifica-tion, audience

targeting criteria, whether the ad was funded through the Google Ad Grants program, a direct link to the ad (creative page url)

The dataset includes an aggregate category for the European Economic Area (EEA). Because EEA-level observations represent aggregated data across multiple countries, including them alongside individual regions would lead to double counting of ads. To avoid this issue, all observations corresponding to the EEA aggregate were excluded from the analysis. The dataset used for subsequent analyses has 1220 unique ad creatives and 7,359 ad instances (6,916 from the "IsraeliGovernment Advertising Agency" and 443 from the "Israel's Government Advertising Agency") across regions and platform surfaces (i.e., Search, Maps, Shopping, and YouTube). All ads are originating from Israel

3.2 MANUAL LABELLING OF AD THEMES

To enable a more precise thematic analysis, we manually labelled each unique ad creative. For each ad:

1. the corresponding creative page url was accessed,
2. the content (video, image, or text) was reviewed and translated if needed.
3. a thematic label was assigned.

Out of the 1,220 creatives, 1,211 ads were successfully labelled (99.3%). A small number could not be accessed due to broken links or unavailable content, therefore we adopted the following conventions: a) Ads with inaccessible links were labelled as "None", b) Ads with unavailable video content were labelled as "Video unavailable", and c) When only the title of the ad was available, the theme was inferred (either directly from the title or by matching it to similar ads with known content). For instance, an ad titled "Happy Faces Don't Lie, Hamas Lies" was assigned to the theme "Aid distribution in Gaza", based on its recurrence in other ads clearly associated with this theme.

3.4 MEASUREMENT OF AD EXPOSURE

Impressions are reported as lower and upper bounds. We estimate exposure using the midpoint of these bounds. To capture temporal dynamics, each ad's active interval was expanded into a daily panel where impressions were assumed to be uniformly distributed across active days. As impression data are made publicly available with a delay of 90 days for privacy reasons, a second data collection was conducted after this period to retrieve the missing impression data for the most recent observations. This procedure ensures more complete coverage of exposure across the full study period.

3.5 A FEW EXAMPLES OF ADS

This subsection provides illustrative examples of the types of advertisements included in the dataset. As shown in Figure 1 and Figure 2, advertisements can take different formats within Google's ad-vertising ecosystem, text-based, image-based, and video-based formats. Text-based advertisements typically consist of short written messages designed to convey information or direct users to ex-ternal content, while video-based advertisements combine audiovisual elements to deliver more elaborate narratives. These examples highlight the diversity of formats through which messages are disseminated, which has implications for how information is framed and perceived by users.



Figure 1: Text-based advertisement.

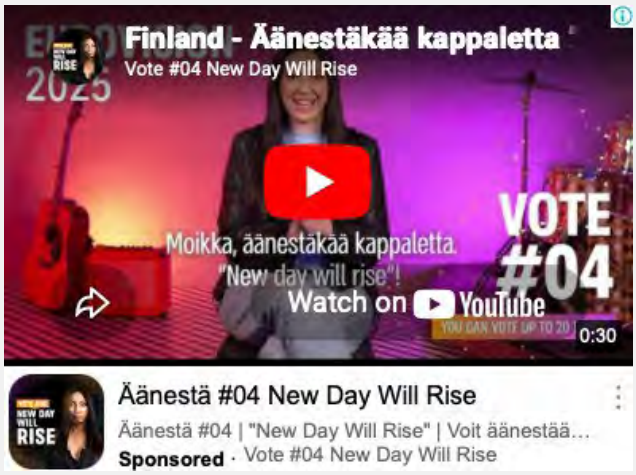


Figure 2: Video-based advertisement.

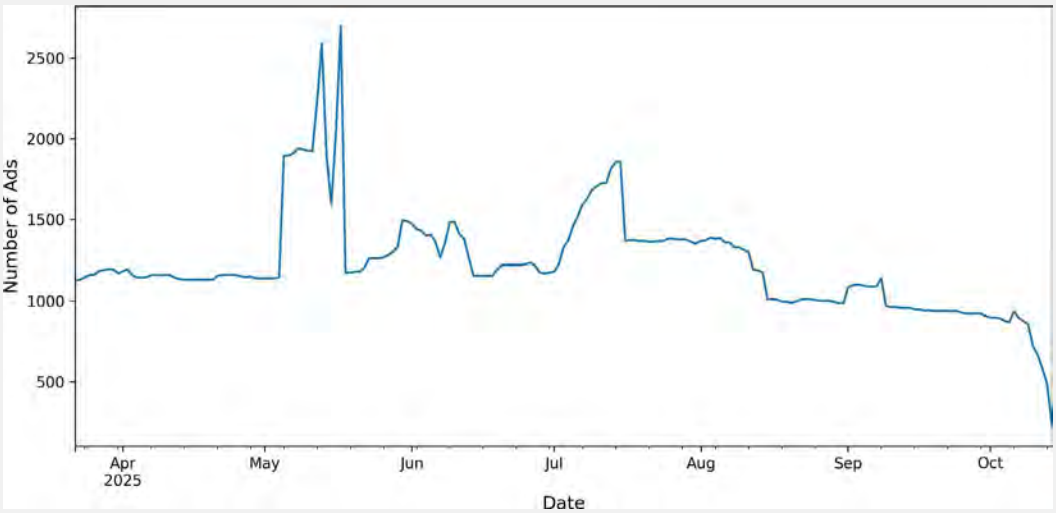


Figure 3: Active Ads per Day (22 March 2025 – 14 Oct 2025)

4. RESULTS

This section presents the empirical findings of the study. It first provides an overview of the Google Ads dataset, including activity levels, formats, and geographic distribution. It then examines the thematic structure of advertisements and their temporal dynamics, before presenting a qualitative analysis of a selected advertisement.

4.1 OVERVIEW OF THE GOOGLE ADS DATASET

This subsection provides a descriptive overview of the dataset. It examines overall advertising activity, the distribution of ads across platform surfaces and formats, geographic targeting patterns, and the platform-assigned topic categories.

4.1.1 Overall advertisement activity

Figure 3 displays the daily number of active advertisement observations between 22 March 2025 and 14 October 2025. The temporal pattern suggests several distinct phases of campaign intensity rather than a uniform distribution over time. After a relatively moderate baseline in late March and April 2025 (approximately 1,100–1,200 active ads), activity increases sharply in early May, reaching peaks above 2,500 active ads. This surge is short-lived, with levels dropping back to around 1,200 shortly thereafter.

Subsequent weeks are characterized by moderate fluctuations, with a secondary increase ob-served in June and a more sustained rise in early July, where activity again approaches higher levels before stabilizing. From August onward, the number of active ads gradually declines, falling to around 1,000 by early September.

Overall, the pattern suggests episodic bursts of intensified advertising activity interspersed with periods of relative stabilization, indicating that the campaign operated in concentrated waves rather than through continuous high-volume deployment. The pronounced decline at the end of the observation window should be interpreted with caution, as the data were collected on 15 October 2025 and the advertising transparency system may not yet reflect all recently active ads due to reporting delays (typically 48–72 hours).

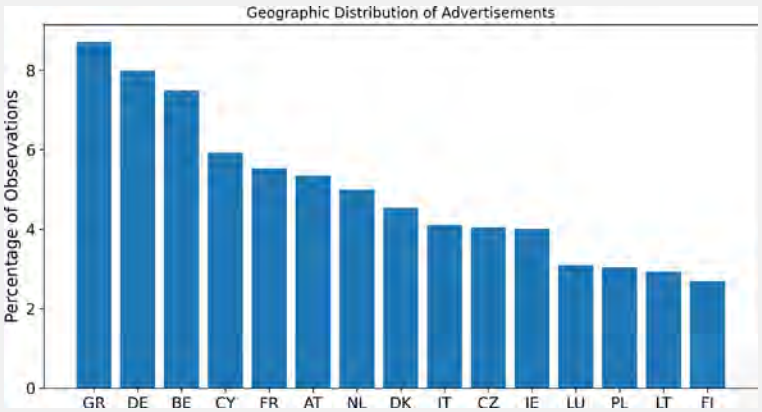


Figure 4: Geographic Distribution of Advertisements (Top 15 locations)

4.1.2 Surface and format distribution

As shown in Table 1, the distribution of advertising surfaces is highly concentrated, with YouTube accounting for the vast majority of estimated impressions. YouTube represents 98.68% of impressions. Other surfaces, contribute more marginally to the advertisement campaign—0.60% in Search, and 0.24% in Maps, Play, and Shopping.

Table 1: Distribution of advertising surfaces by estimated impressions

Surface	Estimated Impressions	Share(%)
YouTube	283,218,500	98.68
Search	1,714,500	0.60
Maps	688,500	0.24
Play	688,500	0.24
Shopping	688,500	0.24

With regard to ad format, video constitutes the dominant format (70.1%), followed by text (24.5%) and image (5.4%). This distribution is consistent with the concentration of impressions on YouTube, showing that advertisers primarily relied on video-based formats to maximize reach and engagement, while text and image ads played a less important role across other surfaces.

4.1.3 Geographic Distribution

The geographic distribution of advertisements reveals a broadly European campaign footprint, with ads spread across a diverse set of national contexts. At the observation level, Greece (8.7%) accounts for the largest share of ads, followed by Germany (8.0%) and Belgium (7.5%). Cyprus (5.9%), France (5.5%), and Austria (5.3%) also represent significant proportions, indicating a strong presence in both central and peripheral regions of Europe. A second tier of countries including the Netherlands (5.0%), Denmark (4.5%), Italy (4.1%), the Czech Republic (4.0%), and Ireland (4.0%) exhibits relatively comparable levels of exposure. Smaller yet still notable shares are observed in Luxembourg (3.1%), Poland (3.0%), Lithuania (2.9%), and Finland (2.7%). Overall, the distribution suggests a geographically dispersed targeting strategy, with no single country overwhelmingly dominating the campaign.

While this pattern reflects broad regional engagement rather than concentration in only a few markets, the inclusion of Greece and Cyprus among the leading recipients is notable in light of recent social and geopolitical developments in the Eastern Mediterranean. Following the escalation of regional tensions and especially in the aftermath of the 2025 12-day war between Israel and Iran, significant relocation flows have been reported. Recent press accounts estimate that approximately 10,000 Israelis have moved to Greece since October 2023 [19]. Similarly, Cyprus has reportedly received around 15,000 Israeli nationals recently, accompanied by notable increases in property ac-quisition and long-term settlement activity [18]. At the state level, this social proximity coincides with deepening institutional cooperation.

In late 2025, Israel, Greece, and Cyprus signed a tri-lateral military work plan for 2026 aimed at intensifying joint exercises and strengthening defense coordination in the Eastern Mediterranean [59]. The convergence of migration flows and formal-ized security collaboration provides additional contextual relevance for the visibility of these two countries within the campaign's geographic targeting strategy.

4.1.4 Platform-Assigned Topic Distribution

Table 2: Distribution of Advertisement Topics (Creative-Level)

Topic Category	Percentage (%)
Law & Government	81.86
Arts & Entertainment	4.16
News, Books & Publications	3.23
Jobs & Education	2.35
Home & Garden	1.97
Family & Community	1.97
Food & Groceries	1.83
Health	1.36
Sports & Fitness	0.41
Autos & Vehicles	0.27
Apparel	0.19
Computers & Consumer Electronics	0.14
Hobbies, Games & Leisure	0.14
Finance	0.08
Business & Industrial	0.04

The topical distribution of advertisements (Table 2) reveals an overwhelming concentration in the category Law & Government, which accounts for 81.9% of all ads. All remaining categories represent only marginal shares of the campaign. The next most frequent categories, Arts & Entertainment (4.2%), News, Books & Publications (3.2%), and Jobs & Education (2.4%) each account for less than five percent of advertisements and all other thematic classifications individually remain below two percent.

4.2 THEMATIC CLASSIFICATION OF ADVERTISEMENTS

This subsection presents the results of the manual thematic classification. It first summarizes the main themes identified in the dataset, and then analyzes their temporal evolution based on estimated impressions and ad activity over time.

4.2.1 Overview of themes

Among the 1220 unique creative ads, we were able to label 1211 of them (7,112 out of 7,359 observations). For the subsequent analyses, advertisements that could not be labelled due to unavailability and which are outside the time frame are excluded. We found a total of 39 unique themes.

Table 3 presents the distribution of manually classified advertisement themes, including both the number of ads and their associated exposure, measured in estimated impressions. Impressions are computed as the sum, across regions, of the midpoint between the reported lower and upper

bounds of impressions for each theme. The distribution of ads is highly skewed, with the "Eurovision vote" category alone accounting for nearly half of all advertisements (47.5%). This dominant category is followed by a substantially smaller group of themes, most notably "Aid distribution in Gaza" (13.3%) and "National Insurance (Hebrew)" (7.7%), while all remaining categories individually account for less than 6% of observations. Beyond these leading themes, the distribution becomes increasingly fragmented, with a long tail of low-frequency categories, many of which represent less than 1% of the dataset.

However, this pattern differs markedly when considering exposure. In terms of estimated impressions, "Aid distribution in Gaza" emerges as the most prominent theme (38.7%), slightly exceeding "Eurovision vote" (36.9%), despite having substantially fewer ads. This contrast indicates that advertisements within the "Aid distribution in Gaza" category were, on average, shown more intensively than those in the "Eurovision vote" category. Similarly, several themes with relatively few ads—such as "UN refuses to distribute the aid to Gaza" or "Gaza lacking food is a lie"—account for disproportionately large shares of total impressions.

These differences highlight a clear distinction between the volume of advertisements and their effective reach. While some themes rely on a large number of creatives and ad instances, others achieve high exposure with comparatively fewer ads, suggesting variation in campaign intensity and distribution strategies across themes."National Insurance (Hebrew)" (7.7%), while all remaining categories individually account for less than 6% of observations. Beyond these leading themes, the distribution becomes increasingly fragmented, with a long tail of low-frequency categories, many of which represent less than 1% of the dataset.

4.2.2 Thematic impressions over time

Figure 5 presents the temporal evolution of advertisement exposure by theme, measured in esti-mated daily impressions and displayed on a logarithmic scale. Impressions are estimated as the midpoint between the reported lower and upper bounds and are distributed uniformly across the active period of each advertisement.

The results reveal substantial variation in exposure across themes and over time. Peaks in the time series indicate periods of intensified campaign activity, while the logarithmic scale highlights differences across both

high-and low-exposure themes. For readability, themes are presented in three groups based on their overall level of exposure.

Table 3: Distribution of Manually Classified Advertisement Themes

Theme	Ads(%)	Creatives	Impressions(%)
Aid distribution in Gaza	953(13.40)	209	132,109,000(38.72)
Eurovision vote	3,380(47.53)	652	126,104,000(36.96)
UN refuses to distribute the aid to Gaza	18(0.25)	18	19,534,500(5.73)
Gaza lacking food is a lie	25(0.35)	17	15,059,500(4.41)
The war can stop if Hamas releases hostages and disarm	100(1.41)	20	14,640,000(4.29)
Hamas stealing aid	60(0.84)	12	7,878,500(2.31)
Famine in Gaza is a lie	20(0.28)	20	6,872,000(2.01)
Dinah project	105(1.48)	21	5,904,500(1.73)
Aid enters Gaza but hostages are starving	59(0.83)	15	3,895,500(1.14)
Against the ICJ	90(1.27)	18	2,567,500(0.75)
Against the Palestinian Authority	30(0.42)	6	2,550,000(0.75)
About Hamas (threatens Israel, should disarm and release hostages)	165(2.32)	33	1,651,000(0.48)
Against UNRWA	185(2.60)	19	584,500(0.17)
Hostages are starving in Gaza	19(0.27)	15	511,500(0.15)
Against UN report and Francesca Albanese	235(3.30)	10	440,500(0.13)
7 October Parliamentary Commission Report (APPG)	5(0.07)	1	425,000(0.12)
Video unavailable	65(0.91)	13	106,000(0.03)
Ministry of Aliyah and Integration	173(2.43)	25	97,500(0.03)
Against Hind Rajab Foundation	390(5.48)	7	77,000(0.02)
Bias in UN reports - Report on the use of human shields by Hamas	10(0.14)	2	66,500(0.02)
Video unavailable - Title: Des milliers de nouvelles recrues du Hamas au cours des derniers mois	25(0.35)	5	59,500(0.02)
Ad for an event in Hebrew	99(1.39)	9	58,500(0.02)
National Insurance (hebrew)	545(7.66)	14	55,500(0.02)
Israeli police is recruiting	68(0.96)	14	24,000(0.01)
Ministry of Education (hebrew)	35(0.49)	5	17,500(0.01)

Flaws of IPC report	7(0.10)	6	8,500(0.00)
Against UNHRC	45(0.63)	2	7,500(0.00)
Ministryof Transportation (safe return to Israel) (hebrew)	70(0.98)	1	7,000(0.00)
Work in prison (hebrew)	20(0.28)	4	6,000(0.00)
National Insurance for reservists (hebrew)	45(0.63)	1	4,500(0.00)
Amit programme (hebrew)	5(0.07)	1	2,500(0.00)
Ministry of Justice (for victims of violence) (hebrew)	20(0.28)	2	2,000(0.00)
Ministry of Defense (hebrew)	2(0.03)	1	1,000(0.00)
Bank of Israel	6(0.08)	2	1,000(0.00)
Israel Land Authority (hebrew)	2(0.03)	2	1,000(0.00)
Protests against Hamas	10(0.14)	2	1,000(0.00)
Ministry of Economy and Industry (hebrew)	10(0.14)	1	1,000(0.00)
National Insurance - Memorial for those who died (hebrew)	10(0.14)	1	1,000(0.00)
Against the Flotilla	11(0.15)	7	0(0.00)

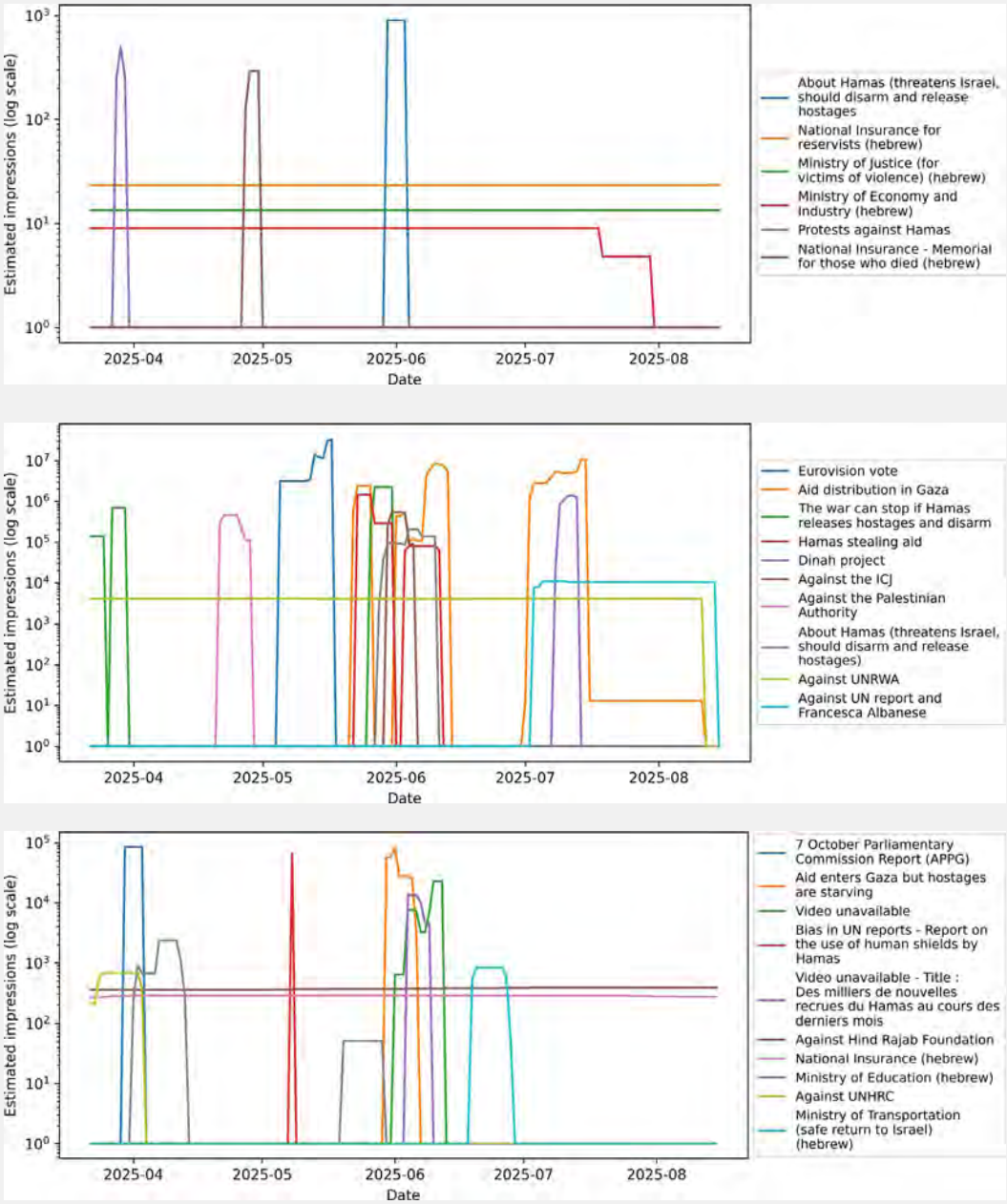


Figure 5: Daily estimated impressions by theme (log scale).

Figures 5 suggest that advertising activity is not only uneven across themes but also highly time-specific, with most themes exhibiting short, concentrated periods of visibility rather than con-tinuous exposure. This pattern indicates that individual themes were likely deployed strategically in response to particular events or moments in the information environment. The clearest example is the “Eurovision vote” theme, which peaks sharply in the weeks preceding the Eurovision Song Contest and disappears immedi-ately thereafter, reflecting a tightly event-driven communication strategy.

A second prominent cluster of themes relates to famine and humanitarian conditions in Gaza. The "Aid distribution in Gaza" theme shows pronounced peaks during the summer of 2025, a period marked by increased international reporting on famine risks and severe food shortages linked to the blockade of the territory. These dynamics have been widely documented by organizations such as the Integrated Food Security Phase Classification and the United Nations, which warned of acute malnutrition and potential famine conditions. In parallel to these reports, several advertising themes appear to contest or reframe this narrative, including "Hamas stealing aid" and messages emphasizing that hostages are the primary victims of deprivation (Aid enters Gaza but hostages are starving"). The temporal alignment of these themes with peaks in humanitarian reporting suggests a reactive communication strategy aimed at shaping interpretations of the crisis.

By contrast, some themes display a more sustained presence over time. Campaigns targeting international organizations—such as those directed against UNRWA, UN reports, or the Inter-national Court of Justice—remain active across much of the observation period, albeit at lower levels of intensity. Similarly, themes associated with governmental institutions (e.g., Ministry of Education, Ministry of Transportation, or National Insurance campaigns) exhibit relatively con-stant, low-level activity, suggesting a background layer of institutional communication rather than episodic mobilization.

More broadly, the figures reveal a dual structure in the campaign's temporal dynamics. On the one hand, high-impression themes are deployed in short, intense bursts tied to specific events or media cycles. On the other hand, a set of lower-intensity themes—often institutional or critical of international actors—remains continuously present.

These patterns raise important questions about the use of online advertising infrastructures for the strategic dissemination of potentially misleading or contested information. While the platform does not classify these advertisements as political, the thematic content and temporal targeting suggest that Google Ads can be used not only for promotion but also for shaping narratives around highly sensitive political and humanitarian issues. In particular, the coexistence of humanitarian reporting on food insecurity in Gaza and advertising themes that contest, reinterpret, or redirect responsibility for these conditions points to the use of advertising as a tool of narrative inter-vention. By leveraging targeted, time-sensitive ad delivery, such campaigns can amplify specific interpretations of events.

4.3 QUALITATIVE ANALYSIS OF AN ADVERTISEMENT

To complement the quantitative findings, this subsection presents an in-depth analysis of a selected advertisement. It illustrates how narratives are constructed and how disinformation can emerge through techniques such as selective quotation, decontextualization, and misleading framing.

We examine an example of an advertisement drawn from the theme "Against the ICJ." The transcript of the ad reads as follows:

Meet the ICJ newest Judge Mahmoud Daifallah Hmoud
"Israel has no right to self-defense"
Those are his words This isn't a judge
It is a prosecutor
He replaces Nawaf Salam Who called Israel an enemy One hostile judge out Another one in
At the ICJ, neutrality is a suggestion Not a requirement
The ICJ has become a political circus The ICJ has lost its legitimacy

At face value, the advertisement presents itself as a factual critique of the ICJ. However, a closer examination reveals that its claims rely on selective quotation, decontextualization, and misleading framing.

First, the statement attributed to Mahmoud Daifallah Hmoud ("Israel has no right to self-defense") is presented without context. According to reporting by Middle East Monitor, Hmoud, speaking as Jordan's representative to the United Nations, argued that Israel does not have the right to invoke self-defense under international law within occupied territories such as Gaza. This legal argument is thus reframed in the advertisement as an absolute and politically motivated position, thereby distorting its original meaning.

Similarly, the reference to Nawaf Salam is misleading. The advertisement claims that he "called Israel an enemy", implying bias incompatible with judicial neutrality. However, this statement appears to derive from Salam's remarks as Lebanese Prime Minister, where he referred to Israel as an "enemy" in the context of the occupation of Lebanese territory and discussions surrounding UN Resolution 1701. As reported by Al Arabiya, these remarks were embedded in a broader political statement concerning ceasefire implementation and territorial withdrawal, rather than an expression of judicial bias. By omitting this context, the advertisement constructs a narrative of systematic hostility within the Court.

Through these selective representations, the advertisement advances a broader claim that the ICJ is inherently biased and lacks legitimacy. This conclusion is not supported by the evidence presented but instead emerges from the cumulative effect of decontextualized and strategically framed statements. Such techniques are characteristic of disinformation practices, where factual elements are not fabricated outright but are manipulated in ways that mislead audiences about their meaning and implications.

The implications of this messaging are particularly significant given the role of the ICJ as the principal judicial organ of the United Nations. At the time of the campaign, the Court was engaged in proceedings concerning allegations of violations of international law in Gaza, including a case brought under the Genocide Convention. In this context, efforts to undermine the perceived neutrality and legitimacy of the Court can be interpreted as attempts to shape public perceptions of ongoing legal processes.

According to the impression bounds reported by the advertising platform, this advertisement was shown between approximately 2.39 and 2.75 million times, indicating a very high level of exposure. Such scale suggests that the message was not marginal but instead widely disseminated, increasing its potential impact on public perceptions. In the context of the preceding analysis, this level of reach reinforces the argument that Google Ads can serve as a powerful vector for the diffusion of disinformation, particularly when deployed in a targeted and time-sensitive manner.

DISCUSSION

This study set out to examine how Google's advertising platform is used as an instrument of information influence, as well as the characteristics and content of these campaigns. The results provide several insights into both the strategic deployment of advertising and its implications for contemporary disinformation.

First, the temporal patterns observed in the data indicate that many advertising campaigns are not continuously deployed but instead activated in short, concentrated bursts aligned with specific events. Themes such as the "Eurovision vote" or narratives surrounding food insecurity in Gaza exhibit clear peaks that coincide with moments of heightened public attention. This finding di-rectly addresses the first research question and is consistent with theories of information influence that emphasize timing and salience, whereby actors intervene precisely when audiences are actively seeking information and are therefore more susceptible to framing effects [45, 23]. In addition to these short-term surges, other themes—such as those targeting UNRWA or the Hind Rajab Foun-dation—display more sustained activity over longer periods, suggesting a complementary strategy of continuous narrative reinforcement.

Second, addressing the second research question, the geographic distribution of advertisements reveals a broad and multi-country targeting strategy across Europe. Rather than concentrating on a single national audience, campaigns were disseminated across multiple regions simultaneously, indicating an attempt to shape international public opinion. This transnational targeting is consis-tent with the logic of hasbara and external communication strategies aimed at influencing foreign publics [8, 39]. It also reflects the affordances of digital advertising systems, which enable precise geographic targeting at scale.

Third, the analysis of impression data shows that exposure is highly concentrated across themes and reaches very large audiences, with some

advertisements being displayed several million times. This concentration of visibility aligns with the auction-based logic of Google Ads, where budget allocation and bidding strategies allow actors to amplify specific messages at scale [6, 32]. At the same time, the data reveal patterns of high-frequency repetition, either through short bursts of intense exposure or through sustained, lower-intensity repetition over longer periods. These dynamics are particularly important in light of the illusory truth effect, whereby repeated exposure increases perceived credibility [37, 5]. In this sense, advertising campaigns do not merely reach large audiences but also repeatedly expose users to the same narratives, reinforcing their potential impact.

Fourth, the qualitative analysis provides insight into the content and construction of these advertisements. The examined example demonstrates how disinformation can be produced not through outright fabrication, but through selective quotation, decontextualization, and misleading framing. Statements are extracted from their original legal or political context and reassembled into a narrative that questions the legitimacy of international institutions such as the ICJ. This corresponds to what the literature describes as malinformation or misleading content, which is particularly difficult to regulate because it relies on partially accurate information [73]. These findings directly address the third research question by showing how narratives are constructed and how meaning is strategically shaped.

Taken together, these results suggest that Google Ads can function as a hybrid instrument of public diplomacy and disinformation. While potentially compliant with platform policies—particularly due to the narrow definition of political advertising related to elections—the campaigns analyzed here operate in a gray zone of issue-based communication. This highlights a gap between plat-form governance frameworks and the broader informational impact of such content, as politically consequential narratives may circulate widely without triggering stricter regulation [34, 33].

More broadly, this study extends existing research on disinformation, which has primarily fo-cused on social media manipulation and coordinated inauthentic behavior [14]. It shows that paid advertising infrastructures constitute an additional and understudied vector of influence. Un-like organic content, search advertising allows actors to insert messages directly at moments of information-seeking, where users are more likely to trust and rely on the information they encounter [55, 26]. This creates conditions under which initial exposure can shape subsequent interpretation, reinforcing the persistence of misleading narratives even in the presence of corrective information [45].

CONCLUSION

This article has examined how Google's advertising infrastructure can be used as a tool of state-linked information influence through the case of Israeli government campaigns. By combining quantitative analysis of advertising data with qualitative examination of message content, the study

demonstrates how digital advertising systems enable both large-scale dissemination and strategic framing of politically sensitive narratives.

The findings show that these campaigns are characterized by targeted temporal deployment, transnational geographic reach, and highly concentrated exposure, often reaching millions of users. They also demonstrate how advertising content can rely on techniques associated with disinfor-mation, including selective framing and decontextualization, to shape interpretations of contested issues.

These results have several implications. First, they suggest that disinformation research should move beyond a narrow focus on social media and incorporate the role of search and advertising systems as key infrastructures of visibility and influence. Second, they point to limitations in current platform governance, particularly the distinction between election-related political advertising and broader issue-based communication. Third, they highlight the importance of transparency tools such as Google's Ads Transparency Center, while also revealing their limitations, including delayed reporting and incomplete data.

Overall, this study contributes to a growing body of work on digital information environments by showing that advertising is not only a commercial tool but also a strong instrument of infor-mation influence. As such, it raises broader questions about platform responsibility, democratic accountability, and the regulation of visibility in the digital public sphere.

REFERENCES

1. Waqas Ahmad et al. Companies inadvertently fund online misinformation through advertising.
2. Nature, 2024. Evidence on advertising financing of misinformation supply chains.
3. Al Jazeera Centre for Studies. Digital occupation: Pixelated propaganda, censored platforms, and the battle for narrative in gaza, 2024. Accessed 2025-12-12.
4. Al Jazeera Media Institute. Information warfare and the battle over gaza's narrative, 2024. Accessed 2025-12-12.
5. Al-Shabaka: The Palestinian Policy Network. Israel's disinformation apparatus: A key weapon in its arsenal, 2022. Accessed 2025-12-12.
6. Gordon W. Allport and Leo Lepkin. Wartime rumors of waste and special privilege: Why some people believe them. Journal of Abnormal and Social Psychology, 40(1):3–36, 1945.
7. Alphabet Inc. Form 10-k for fiscal year ended december 31, 2024 (sec filing). https://www.sec.gov/Archives/edgar/data/1652044/000165204425000014/goog-20241231.htm, February 2025. Business description and revenue discussion for Google Services advertising.
8. Amnesty International. Amnesty international report on genocide in gaza. https://web.ar chive.org/web/20250724065956/https://amnesty.ca/wp-content/uploads/2024/12/Am nesty-International-Gaza-Genocide-Report-December-4-2024.pdf, December 2024.
9. Miriyam Aouragh. Hasbara 2.0: Israel's public diplomacy in the digital age. Middle East Critique, 25(3):271–297, 2016.
10. David S Ardia, Evan Ringel, Victoria Ekstrand, and Ashley Fox. Addressing the decline of local news, rise of platforms, and spread of mis-and disinformation online: A summary of current research and policy proposals. UNC Legal Studies Research Paper, 2020.
11. William Audureau, Samuel Forey, and Assma Maad. "quarante b´eb´es d´ecapit´es": itin´eraire d'une rumeur au cœur de la bataille de l'information entre isra¨el et le hamas, April 2024. Accessed 2025-12-12.
12. L´ıvia Benkov´a. The rise of russian disinformation in europe. Austria Institut fu¨r Europa und Sicherheitspolitik, 2018.
13. Jonah Berger. Arousal increases social transmission of information. Psychological science, 22(7):891–893, 2011.
14. Samantha Bradshaw and Philip N. Howard. The global disinformation order: 2019 global inventory of organised social media manipulation. Technical report, Oxford Internet Institute, 2019. Accessed 2025-12-16.
15. Samantha Bradshaw and Philip N. Howard. Industrialized disinformation 2020 global inventory of organized social media manipulation. Technical report, Oxford Internet Institute, University of Oxford, 2020. Accessed 2025-12-17.
16. Michal- Chora´s, Konstantinos Demestichas, Agata Giel-czyk, A´lvaro Herrero, Pawel-Ksieniewicz, Konstantina Remoundou, Daniel Urda, and Michal- Wo´zniak. Advanced machine learning tech-niques for fake news (online disinformation) detection: A systematic mapping study. Applied Soft Computing, 101:107050, 2021.
17. Matteo Cinelli, Gianmarco De Francisci Morales, Alessandro Galeazzi, Walter Quattrociocchi, and Michele Starnini. The echo chamber effect on social media. Proceedings of the National Academy of Sciences of the United States of America, 118(9):e2023301118, 2021. Accessed 2025-12-12.
18. Ellen M Cotter. Influence of emotional content and perceived relevance on spread of urban legends: A pilot study. Psychological reports, 102(2):623–629, 2008.
19. The Cradle. Cyprus: Netanyahu's new haifa. The Cradle, 2025.

20. La Croix. Loin de la ¨terre promise¨et de la guerre, ces isra´eliens qui s'installent en gr`ece. La Croix International, 2025.
21. Nicholas John Cull. Propaganda and Mass Persuasion: A Historical Encyclopedia, 1500 to the Present. ABC-CLIO, 2003.
22. Carlos A. D´ıaz Ruiz et al. Disinformation and fake news as externalities of digital advertising markets. Journal of Marketing Management, 2024. Discusses how advertising market incentives can sustain harmful information ecosystems.
23. Drop Site News. Google's $45 million contract with netanyahu's office to spread israeli pro-paganda. https://www.dropsitenews.com/p/google-youtube-netanyahu-israel-propaganda-gaza-famine, September 2025.
24. Ullrich K. H. Ecker, Stephan Lewandowsky, John Cook, Philipp Schmid, Lisa K. Fazio, Nadia Brashier, Panayiota Kendeou, Emily K. Vraga, and Michelle A. Amazeen. The psychological drivers of misinformation belief and its resistance to correction. Nature Reviews Psychology, 1:13–29, 2022.
25. Allen L Edwards. The relationship between the judged desirability of a trait and the probability that the trait will be endorsed. Journal of applied Psychology, 37(2):90, 1953.
26. Allen L Edwards. The social desirability variable in personality assessment and research.
27. Dryden Press, 1957.
28. Robert Epstein and Ronald E. Robertson. The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections. Proceedings of the National Academy of Sciences, 112(33):E4512–E4521, 2015.
29. European External Action Service. Euvsdisinfo, 2023. Accessed 2025-12-12.
30. European External Action Service. Second eeas report on foreign information manipulation and interference threats. Technical report, EEAS, 2023. Accessed 2025-12-16.
31. Jean-Pierre Filiu. Anatomy of an israeli disinformation campaign, July 2024. Accessed 2025-12-12.
32. Richard Fletcher, Alessio Cornia, Lucas Graves, and Rasmus Kleis Nielsen. Measuring the reach of" fake news" and online disinformation in europe. Australasian Policing, 10(2):25–33, 2018.
33. Nathaniel Gleicher. Removing coordinated inauthentic behavior from israel, 05 2019. Accessed 2025-12-17.
34. Google. How the google ads auction works / ad rank. https://support.google.com/google-ads/answer/6366577?hl=en, 2025. Documentation describing auction-based placement and Ad Rank factors.
35. Google. Misrepresentation — advertising policies help. https://support.google.com/ads policy/answer/6020955?hl=en, 2025.
36. Google. Political content — advertising policies help. https://support.google.com/adspo licy/answer/6014595?hl=en, 2025.
37. Google Business. Ai-powered search marketing. https://business.google.com/us/think
38. /search-and-video/ai-powered-search-marketing/, 2025. Accessed 2025-12-17.
39. Andrew M Guess and Benjamin A Lyons. Misinformation, disinformation, and online propaganda. Social media and democracy: The state of the field, prospects for reform, 10:10–33, 2020.
40. Lynn Hasher, David Goldstein, and Thomas Toppino. Frequency and the conference of refer-ential validity. Journal of Verbal Learning and Verbal Behavior, 16(1):107–112, 1977.
41. Chip Heath, Chris Bell, and Emily Sternberg. Emotional selection in memes: the case of urban legends. Journal of personality and social psychology, 81(6):1028, 2001.
42. Bernd Hirschberger. External Communication in Social Media During Asymmetric Conflicts. transcript Verlag, 2021.

43. Simon Hooper and Dania Akkad. Israel–palestine war: How unverified reports of hamas 'beheading babies' filled front pages, October 2023. Accessed 2025-12-12.
44. i24NEWS. 'it smells of death' here — surveying the scenes of atrocities in kfar aza, 2023. Accessed 2025-12-12.
45. Institute for Middle East Understanding. Fact sheet: Israel's history of spreading disinforma-tion, 2023. Accessed 2025-12-12.
46. Alexander Lanoszka. Disinformation in international politics. European journal of interna-tional security, 4(2):227–248, 2019.
47. David MJ Lazer, Matthew A Baum, Yochai Benkler, Adam J Berinsky, Kelly M Greenhill, Filippo Menczer, Miriam J Metzger, Brendan Nyhan, Gordon Pennycook, David Rothschild, et al. The science of fake news. Science, 359(6380):1094–1096, 2018.
48. Stephan Lewandowsky, Ullrich K. H. Ecker, and John Cook. Misinformation and its correction: Continued influence and successful debiasing. Psychological Science in the Public Interest, 13(3):106–131, 2012. Accessed 2025-12-12.
49. Volodymyr Lysenko and Catherine Brooks. Russian information troops, disinformation, and democracy. First Monday, 2018.
50. Diego A Martin, Jacob N Shapiro, and Michelle Nedashkovskaya. Recent trends in online foreign influence efforts. Journal of Information Warfare, 18(3):15–48, 2019.
51. Alice Marwick and Rebecca Lewis. Media manipulation and disinformation online. New York: Data & Society Research Institute, 359:1146–1151, 2017.
52. Timothy P McGeehan. Countering russian disinformation. The US Army War College Quar-terly: Parameters, 48(1):7, 2018.
53. Dana¨e Metaxa-Kakavouli and Nicol´as Torres-Echeverry. Google's role in spreading fake news and misinformation. Technical report, SSRN, October 2017. Available at SSRN: https://ssrn.com/abstract=3062984.
54. Susan Morgan. Fake news, disinformation, manipulation and online tactics to undermine democracy. Journal of cyber policy, 3(1):39–43, 2018.
55. Bennet B. Murdock. The serial position effect of free recall. Journal of Experimental Psychol-ogy, 64(5):482–488, 1962.
56. Raymond S. Nickerson. Confirmation bias: A ubiquitous phenomenon in many guises. Review of General Psychology, 2(2):175–220, 1998.
57. Organisation for Economic Co-operation and Development. Facts not fakes: Tackling disinfor-mation, strengthening information integrity. Technical report, OECD, Paris, 2024. Accessed 2025-12-16.
58. Bing Pan, Helene Hembrooke, Thorsten Joachims, Lori Lorigo, Geri Gay, and Laura Granka. In Google we trust: Users' decisions on rank, position, and relevance. Journal of Computer-Mediated Communication, 12(3):801–823, 2007.
59. Christopher Paul and Miriam Matthews. The russian "firehose of falsehood" propaganda model. Technical report, RAND Corporation, 2016. Accessed 2025-12-16.
60. Andrea Pereira, Elizabeth Harris, and Jay J. Van Bavel. Identity concerns drive belief: The impact of partisan identity on the belief and dissemination of true and false news. Group Processes & Intergroup Relations, 26(1):24–47, 2023.
61. Kim Peters, Yoshihisa Kashima, and Anna Clark. Talking about others: Emotionality and the dissemination of social information. European Journal of Social Psychology, 39(2):207–222, 2009.
62. The Jerusalem Post. Trilateral work plan for military cooperation between israel, greece, cyprus signed - exclusive. The Jerusalem Post, 2025.

63. Kristen Purcell, Joanna Brenner, and Lee Rainie. Search engine use 2012. Technical report, Pew Research Center, March 2012. Report and topline findings on U.S. search engine use and preferences.
64. Edward W. Said. Propaganda and war. Media Monitors Network, August 2001.
65. Simona Stano et al. The internet and the spread of conspiracy content. In Routledge handbook of conspiracy theories, pages 483–496. Routledge, 2020.
66. Charles S. Taber and Milton Lodge. Motivated skepticism in the evaluation of political beliefs.
67. American Journal of Political Science, 50(3):755–769, 2006.
68. The New Arab. Israel to quadruple hasbara spending in bid to salvage global reputation, 2024. Accessed 2025-12-17.
69. The Washington Post. Google email shows it ruled israel's ads claiming 'there is food in gaza' aren't misleading. https://www.washingtonpost.com/technology/2025/10/15/israel-ads-youtube-famine-gaza/, October 2025. Reports on policy complaints and Google's decision regarding Israel-promoted ads about Gaza famine claims.
70. Craig Timberg and Tony Romm. Facebook shuts down israel-based disinformation campaigns as election manipulation increasingly goes global. The Washington Post, May 2019. Accessed 2025-12-17.
71. Kathie M d'I Treen, Hywel TP Williams, and Saffron J O'Neill. Online misinformation about climate change. Wiley Interdisciplinary Reviews: Climate Change, 11(5):e665, 2020.
72. TRT World. How israel uses disinformation to shape the gaza narrative, 2024. Accessed 2025-12-12.
73. TRT World. Israel pumps millions into a disinformation campaign to deny gaza famine.
74. https://www.trtworld.com/article/26aa3a47f85b, September 2025.
75. United Nations Office for the Coordination of Humanitarian Affairs and Office of the High Commissioner for Human Rights. Special rapporteur report on gaza: Genocide as a collective crime, October 2025. Accessed 2025-12-12.
76. Michela Del Vicario, Alessandro Bessi, Fabiana Zollo, Fabio Petroni, Antonio Scala, Guido Caldarelli, H. Eugene Stanley, and Walter Quattrociocchi. The spreading of misinformation online. Proceedings of the National Academy of Sciences, 113(3):554–559, 2016.
77. Nathan Walter and Riva Tukachinsky. A meta-analytic examination of the continued influence of misinformation in the face of correction: How powerful is it, why does it happen, and how to stop it? Communication research, 47(2):155–177, 2020.
78. Claire Wardle and Hossein Derakhshan. Information disorder: Toward an interdisciplinary framework for research and policymaking. Technical Report 27, Council of Europe, 2017.
79. Jen Weedon, William Nuland, and Alex Stamos. Information operations and facebook, 2017.
80. WIRED. Israel is buying google ads to discredit the UN's top gaza aid agency. https:
81. //www.wired.com/story/israel-unrwa-usa-hamas-google-search-ads/, August 2024. Reports on Israel-linked Google Search ads targeting UNRWA/UNRWA USA queries

ARTIFICIAL INTELLIGENCE IN GAZA'S HUMANITARIAN SYSTEM: **A DECOLONIAL FEMINIST REFLECTION OF CONTROL AND ACCESS**

RAWAN YOUSEF

Abstract	140
Introduction	140
Methodology	144
Findings: AI, Digital Governance, and Everyday	145
Discussion: AI, Governance, and Power in Gaza's Humanitarian System	151
Conclusion and policy implications	152



Rawan is a political scientist and researcher in feminist and decolonial frameworks. She holds an MA in Development Studies from Erasmus University and is currently a Ph.D. candidate in political science at the Hebrew University of Jerusalem. Her work bridges feminist theory, humanitarianism, and decolonial critique, with a strong record of field-based research and mentoring.

Her research examines how AI-driven humanitarian systems shape aid delivery in Gaza, the West Bank, and East Jerusalem. Through a feminist and decolonial lens, she analyzes how digital tools like biometric registration and predictive algorithms embed surveillance and reinforce structural inequalities.

ABSTRACT

This paper examines how artificial intelligence and broader digital systems operate in Gaza-related humanitarian work under conditions of siege, infrastructural destruction, surveillance, and external control. Rather than treating AI as a discrete innovation, it analyzes how humanitarian staff encounter, interpret, and navigate AI-related and digital systems in everyday practice. Drawing on ten qualitative interviews with Palestinian and non-Palestinian humanitarian practitioners, the paper shows that AI appears in two entangled forms: informal staff use of generative tools to manage administrative pressure, and institutional digital systems that structure registration, verification, eligibility, reporting, and the circulation of humanitarian data.

The paper argues that the significance of AI in Gaza is less technical than institutional. AI-related and digital systems function as infrastructures of humanitarian governance that intensify classification, expand data circulation without sovereignty, and redistribute labor, risk, and authority across an unequal operational chain. The findings identify four recurring dynamics: informal adoption under weak governance, externalized control over categories and lists, downward displacement of labor and risk, and everyday negotiation under conditions of care, exposure, and constrained agency.

By bringing together scholarship on humanitarian governance, critical data and AI studies, settler colonial governance, and feminist political economy, the paper reframes AI in humanitarianism away from tool inventories and ethics checklists and toward governance in a colonized humanitarian space. It shows that in Gaza, AI intensifies existing relations of bureaucratic domination, epistemic dependency, and constrained contestability.

Keywords: **artificial intelligence; humanitarian governance; digital aid; Gaza**

INTRODUCTION

Artificial intelligence is increasingly discussed as reshaping humanitarian governance, yet in many operational settings it enters unevenly, informally, and only partially through formal institutional frameworks. In Gaza, AI-related and digital systems appear less as visible organizational innovations than as part of everyday administrative practice, mediated through platforms and procedures designed elsewhere and navigated under severe political and operational constraints. Understanding their role therefore requires shifting attention from institutional design to governance as encountered in practice.

Gaza offers a particularly revealing case. Humanitarian action there operates within a highly restricted environment shaped by blockade, recurring large-scale violence, fragmented authority, and externally mediated access to infrastructure, goods, and financial systems. Coordination, assistance delivery, and eligibility verification increasingly depend on digital platforms, remote management arrangements, and standardized data procedures. Some of these processes involve AI-enabled tools, while many reflect

broader forms of digitalization. Distinguishing between AI and digital governance is therefore analytically necessary.

In this paper, "AI-related systems" refers to tools that incorporate algorithmic processing, automated decision-support, or generative AI functions. "Digital systems" refers more broadly to platform-based coordination tools, registration infrastructures, databases, and administrative technologies that shape humanitarian work without necessarily relying on AI. Not all forms of digitalized humanitarian governance in Gaza are AI-driven, even when they shape access, classification, coordination, and control. The paper therefore examines AI within a wider field of digital governance while remaining attentive to the limits of the available evidence on formal AI deployment.

The paper argues that in Gaza, AI-related and digital systems function less as discrete technological tools than as infrastructures of humanitarian governance. Rather than mapping institutional adoption across the sector, it examines how humanitarian staff encounter, interpret, and navigate these systems in daily work. In Gaza-related humanitarian operations, AI is not primarily a technological development but a governance mechanism that reorganizes legibility, labor, and authority under conditions of colonial constraint. This shifts attention from organizational narratives of innovation to governance enacted through interfaces, procedures, delegated routines, and opaque decision chains.

The paper contributes to debates on humanitarian AI and digital governance by foregrounding everyday practice in a highly constrained political context. Existing scholarship has examined algorithmic governance, data-driven humanitarianism, and the political economy of digital aid systems, but has focused more often on organizational strategy, technological design, or large-scale policy implications than on how such systems are negotiated in practice. Focusing on Gaza, this study shows that AI-mediated and digital governance is lived through administrative labor, interpretive work, risk management, and uneven institutional visibility rather than formal institutional transformation alone.

The analysis is guided by three research questions: How are AI-related and digital systems encountered and navigated by humanitarian staff working in Gaza? Through what institutional and technical mechanisms do these systems shape humanitarian coordination, decision-making, and assistance delivery? How do humanitarian actors interpret, negotiate, and contest AI-mediated governance under conditions of political and operational constraint?

To address these questions, the paper draws on qualitative interviews with humanitarian practitioners working in Gaza across international and local organizations, complemented by contextual analysis of organizational and policy materials. The findings show that AI-related and digital systems function as everyday governance infrastructures embedded in administrative routines, platform dependencies, and verification processes, while frontline actors negotiate them under conditions of uncertainty, asymmetrical technological control, and heightened political risk.

This paper proceeds in five parts. The next section sets out the analytical framework, followed by the methodology. The findings chapter presents empirical analysis through four recurring dynamics: informal adoption under weak governance, externalized control over categories and lists, downward displacement of labor and risk, and everyday negotiation under conditions of care, exposure, and constrained agency. The discussion situates these findings within wider debates on humanitarian governance and technological power, and the conclusion reflects on their broader policy implications.

ANALYTICAL FRAMEWORK: HUMANITARIAN AI, DIGITAL GOVERNANCE, AND COLONIAL POWER

Research on humanitarian AI and digital governance shows that technologies introduced in the language of efficiency and innovation often reorganize authority and accountability in less visible ways. AI-supported systems can narrow interpretive space, embed judgment in opaque infrastructures, and make decisions harder to contest, while digital systems privilege standardization and measurable outputs over contextual judgment (Coppi et al. 2021; Burrell 2016; Ananny and Crawford 2018; Devidal 2024). Where consent, refusal, and recourse are weak, they may amplify harm rather than reduce it (Beduschi 2022; Latonero 2019; Weitzberg et al. 2021). AI is therefore treated here not primarily as a toolset but as part of a wider field of digital governance shaping classification, verification, and decision-making.

This must be situated in Gaza's specific political and material context. Humanitarian action there operates under blockade, occupation, infrastructural destruction, restricted movement, fragmented authority, and externally mediated access to goods, infrastructure, and financial systems. Digital and AI-related systems do not enter a neutral administrative space. They operate within an existing architecture of surveillance, documentation, classification, and constrained institutional agency. The question is therefore not simply whether AI is used, but how AI-related and digital systems are encountered within a broader regime of humanitarian governance under colonial constraint.

Scholarship on humanitarian and bureaucratic governance helps clarify this. Aid increasingly operates through remote management, standardized categories, digital reporting, and rule-based administration rather than direct accountability (Donini and Maxwell 2013; Duffield 2007). Registration and verification systems do not simply identify need. They construct legitimate beneficiaries and produce exclusion where lives do not fit administrative templates (Jacobsen 2015). Technological systems must therefore be understood within ordinary bureaucratic practice, where coordination, eligibility, verification, and delivery appear technical but carry distributive and political effects.

Critical data and AI scholarship further shows how these systems reproduce asymmetrical power through infrastructures, categories, and epistemic authority. Algorithmic opacity stems not only from technical complexity but from the institutional arrangements in which data and models operate (Burrell 2016; Ananny and Crawford 2018). Couldry and Mejias (2019a;

2019b) describe contemporary data extraction as a colonial formation, while Birhane (2020) shows how Global North AI systems rely on extractive practices and imposed classificatory logics that reproduce dependency rather than local agency. In Gaza, where local actors do not control infrastructures, data pathways, or standards, technical systems reorganize legibility, decision-making, and access even when those subject to them have little visibility into how they work.

Settler colonial and colonial governance scholarship provides the broader political structure within which these systems must be read. Wolfe (2006) frames settler colonialism as an ongoing structure of elimination, containment, and management, while Feldman (2008) shows how Gaza has long been governed through documents, permits, categories, and administrative uncertainty. Said (1978) adds that power depends not only on coercion but on institutions that define what is knowable and governable. Registration, verification, categorization, and coordination in Gaza therefore cannot be treated as neutral procedures. They are embedded in pre-existing relations of bureaucratic domination over mobility, legibility, and access.

This matters especially because humanitarian digital infrastructures now operate where donor oversight, private vendors, and security logics are increasingly entangled. Legal and policy scholarship has begun to recognize civilian data as politically consequential in armed conflict, while warning that data protection remains underdeveloped despite growing dependence on centralized digital systems (ICRC 2021; Geiss 2021). Research on humanitarian data governance further shows that personal data collected for aid delivery circulates within wider ecosystems shaped by donors, contractors, states, and security concerns, especially where affected populations have limited means of contestation (GPPi 2021; Grote 2025). In Gaza, humanitarian digital infrastructures do not sit outside security architectures. They operate within an environment saturated by them.

Feminist political economy adds a final layer by showing how governance systems redistribute labor, risk, and responsibility rather than simply improving efficiency. Fraser (2016) and Eubanks (2018) show how care and distribution are turned into technical administration while accountability is displaced onto those who absorb the consequences. In Gaza, these burdens are lived through unpaid care, household survival, documentation, follow-up, and repeated navigation of aid systems under siege and displacement, often by women. Feminist data scholarship also shows that data systems encode normative assumptions about households and eligibility that can misrecognize or exclude those who do not fit standardized categories (D'Ignazio and Klein 2020). Digital governance in Gaza must therefore be read not only as a question of technology and control, but also of social reproduction, dignity, and unevenly distributed labor.

To this end, this framework advances three propositions. First, AI-related and digital systems in Gaza function as infrastructures of governance rather than neutral tools. Second, they operate within a colonized space shaped by siege, occupation, and bureaucratic control. Third, they are mediated through everyday labor, interpretation, and uneven forms of negotiation and resistance. Used as an analytical lens rather than a normative model, this

framework allows the paper to examine how such systems redistribute legibility, labor, authority, and responsibility in humanitarian work on Gaza.

METHODOLOGY

This study adopts a qualitative interpretive case-study design focused on how humanitarian staff working on Gaza encounter, understand, and navigate AI-related and digital systems in practice. Rather than mapping all tools or reconstructing their internal design, it examines technological governance through administrative routines, platform dependencies, verification procedures, institutional caution, and uneven uptake.

DATA, SAMPLING, AND FIELD ACCESS

Primary data consists of ten semi-structured interviews conducted between December 2025 and January 2026 with Palestinian staff inside Gaza, Palestinian staff displaced to or operating from Egypt, and non-Palestinian staff from UN agencies and international NGOs in operational and managerial roles. More than fifty interview requests were sent across UN agencies, INGOs, and local Palestinian NGOs; many received no response, were redirected to headquarters, or were declined due to institutional sensitivity. Participants were selected purposively to capture variation in role, organization, location, and proximity to AI-related and digital practice. The sample is not statistically representative but is used to generate an analytically grounded account of how such systems are experienced and negotiated across institutional positions. Given the sensitivity of Gaza-related humanitarian work, all interviews were conducted anonymously, with oral consent, generalized affiliations and roles, and participant-defined boundaries to reduce risk. Some system names, workflows, and institutional procedures are withheld as ethical necessities. Because war, displacement, infrastructural collapse, and security constraints limited access to system design, donor decision-making, and military-controlled data infrastructures, the study draws selectively on humanitarian policy documents, technical guidance, public program descriptions, and reports as contextual and interpretive support rather than as a co-equal method.

Analytic Procedure

The analysis is guided by the paper's integrated framework on humanitarian governance, critical data and AI studies, settler colonial governance, and feminist political economy. These perspectives informed the interview guide and oriented analysis toward recurring themes such as classification, access, administrative discretion, verification, opacity, labor redistribution, and institutional risk. Interview material was analyzed thematically, following Braun and Clarke, through iterative coding and comparative reading across participants to identify patterned mechanisms and meaningful variation in how AI-related and digital systems were encountered in practice. Attention was given to gaps between formal institutional claims and everyday operational experience. Secondary materials were used only to contextualize and interpret interview accounts where relevant, not as independent evidence for broad claims about internal system design or sector-wide deployment.

Positionality and Reflexivity

This research is conducted by a Palestinian woman researcher working in close proximity to the humanitarian context under study and occupying a position of partial insiderhood alongside critical distance. Shared language and lived experience of occupation, and familiarity with humanitarian institutions supported access and interpretation, while reflexivity was maintained throughout to avoid over-identification and remain attentive to differences in role, exposure, and the limits of representation under war and political constraint.

Limitations and Credibility

The study is based on a limited number of interviews and does not claim representativeness across the humanitarian sector. Access was constrained by gatekeeping, security concerns, and redirection to organizational headquarters, and the research could not directly observe system design, backend operations, donor decision-making, or military-controlled data infrastructures. It therefore examines how humanitarian staff encounter, interpret, and navigate AI-related and digital systems in practice, rather than the full institutional architecture behind them. Credibility rests on the coherence of patterns across participants in different roles, locations, and organizational positions, with broader claims limited to what can be supported by interview data and publicly available contextual material.

FINDINGS: AI, DIGITAL GOVERNANCE, AND EVERYDAY HUMANITARIAN PRACTICE IN GAZA

Across the interviews, "AI" appears in two entangled forms: informal staff use of generative tools to manage workload, and broader digital systems governing registration, verification, eligibility, reporting, and data circulation (Interviews 2, 4, 5, 8, 10). The findings center on four recurring dynamics: informal adoption under weak governance, externalized control over categories and lists, downward displacement of labor and risk, and everyday negotiation under conditions of care, exposure, and constrained agency.

The interviews show that AI-related and digital systems enter Gaza-related humanitarian work unevenly through routine practice, platform dependencies, verification processes, and administrative coping. Their most consistent effects are not innovation or efficiency, but intensified classification work, partial visibility, expanded data exposure, and uneven burdens of verification, reporting, and compliance.

1. Informal AI Use and Governance through Silent Permission

AI enters everyday humanitarian work primarily as a coping tool rather than a formal innovation project. Across roles, interviewees described using generative tools to manage workload, compress administrative labor, and sustain performance under crisis conditions. One interviewee explained: "I use everything that is useful for me… Blackbox, Gemini, any programming helping… I want to make things easier for myself" (Interview 2). The same participant linked this directly to performance and managerial expectations: "since I started to use AI, my manager is happier with me… my work

improved... I use it as my personal assistant" (Interview 2). In finance work, AI was similarly framed as reducing micro-level cognitive labor: "instead of thinking about a formula in excel... I ask AI to do the work" (Interview 3). Across these accounts, AI appeared less as strategic institutional transformation than as an informal survival tool within overburdened humanitarian labor regimes (Interviews 2, 3, 8, 10).

At the same time, its use was materially uneven. A Gaza-based case manager described AI as available only when infrastructure allowed, and unreliable even then: "I only have stable internet in the office, I use ChatGPT, but I have a lot of difficulties. ChatGPT deletes my original points or just change important information" (Interview 10). She tied these limits directly to fieldwork, care work, and infrastructural collapse: "my work is mostly in the field, I cannot focus, I need to take care of meals, my children, the house duties with no much electricity or much anything, I don't have time for AI" (Interview 10). Others expressed open skepticism, especially in local NGO settings where AI was read less as opportunity than as vulnerability. One practitioner said simply: "We are worried of it. that should be prohibited. Completely" (Interview 4). Another argued that AI use in Gaza was "not mature enough" under current conditions and required close monitoring of consequences and impact (Interview 1). AI uptake therefore appears stratified by role, organizational policy, connectivity, and the lived conditions of siege rather than evenly distributed across the humanitarian system.

A second pattern was the mismatch between formal authorization and actual practice. Staff repeatedly described AI use as unofficial, quietly tolerated, selectively prohibited, or simply left undefined. One Gaza-based practitioner stated this directly: "We use other tools for the thinking part and decision-making processes, officially, we are not allowed, but unofficially, we use some of these tools to help extract patterns from data, and to make decisions and recommendations" (Interview 5). Another described widespread use of unauthorized tools for decision-adjacent work: "Many staff use AI tools outside official or authorized channels... colleagues often upload Excel sheets or databases containing personal data into tools like ChatGPT and ask them to conduct scoring, determine eligibility criteria, or generate recommendations" (Interview 5). At the local NGO level, this often appeared as governance through absence. As one case manager explained, "No one in my organization told me what I should or should not [do] I use it when it's convenient" (Interview 10).

Across interviews, this produced a pattern of organizational silence, partial rules, and uneven enforcement in which informal AI use expanded while responsibility remained individualized. The contrast with more formal ICT governance structures is instructive. One interviewee working on governance and permissions emphasized that some AI tools were explicitly unauthorized because weak permissions could make sensitive information visible to "unexpected and unauthorized users" (Interview 6). Yet even there, governance appeared fragile because it depended on technical maturity, staff awareness, and enforceable boundaries that were uneven in practice.

2. Classification, Verification, and the "User" Position

The second finding is that the most consequential site of AI-adjacent governance is not innovation, but the classification and verification architecture through which access to aid is organized. Interviewees repeatedly described humanitarian work as structured by lists, forms, platform-based registration, scoring processes, and verification chains. Within this architecture, Palestinian local actors are often positioned as operational "users" of systems they do not design, govern, or fully understand.

One local NGO staff member working with a UN agency described this clearly: "the entire online and platform is theirs, and we are there as users" (Interview 4). He explained that local actors had no authority to modify data structures or decide what information was collected: "We don't have specific access to modify or decide on type of information collected… we have no access or control" (Interview 4). Training was provided, but governance was not shared: "[a UN agency] will introduce us to the system, provide technical trainings [so we can] enter data and upload. Behind that we have no access or control" (Interview 4). A Gaza-based case manager described a similar arrangement with another UN agency and an INGO partner: "The UN gives us exactly the lists of people who we should work with… we verify lists… register all information and provide that back" (Interview 10). She located her role as verification labor within a wider system whose outputs remained only partly visible: "UN agencies used this information to produce maps and reports… some information is published and other information are kept, we don't know" (Interview 10). Together, these accounts show that technical access is granted without meaningful governance authority.

This "user" position is not only about platforms, but about how eligibility and access are governed through classification work. Several interviews described aid as operating through externally generated lists, self-registration forms, cross-checking, identity verification, and forms of scoring or recommendation. At one local NGO interface with [a UN agency], digitization was framed through self-registration and vetting: "There is the self-registration form, where beneficiaries register… [we] be a bridge between us as local NGO and the beneficiaries" (Interview 4). The same participant emphasized the pressure of verification under scarcity: "our problem is that some people used to deceive us through registration, we thus need to verify, also we use clusters data but our capacity to do cross checking and vetting is very limited." Survival thus becomes entangled with category navigation while local actors remain responsible for verifying need through administrative templates they did not design.

The interviews also suggest that AI can enter this classification architecture informally and consequentially. One participant described colleagues uploading Excel sheets or databases into AI tools in order to "conduct scoring, determine eligibility criteria, or generate recommendations" (Interview 5). Another warned that AI-generated recommendations could distort needs assessment by inventing or confusing key categories: "major issues on how AI interpretates the data… it always mixes between quantities and measurements also numbers and distances, family members, sex etc. and it can create or generate data that wasn't there to fill gaps" (Interview 2). A case manager further described the routine chain of external list production and

local verification: "I receive lists from [a UN agency] we verify lists of beneficiaries, visit children and family, check that they are the actual people as per the vetted lists and ID numbers" (Interview 10). These accounts indicate that access is shaped through opaque chains of categorization, vetting, and verification in which machine-assisted reasoning may enter through ordinary staff practice rather than visible system rollout.

Across these interviews, local actors carry the burden of data production and verification while authority over classification, interpretation, and downstream visibility remains external.

3. Data Exposure, Labor Displacement, and Infrastructural Constraint

The third finding is that AI-related and digital governance in Gaza displaces labor and risk downward under conditions of severe infrastructural fragility. Participants described data not as neutral administrative material but as politically dangerous. The issue was not only privacy in the abstract, but the exposure of Palestinian data within a securitized environment and the inability of local actors to know, control, or contest where data travels after collection.

One local NGO practitioner put this plainly: "First and foremost the security of the data" (Interview 4). He linked this to vetting and exclusion, expressing fear of "decision making or vetting that is based on machine learning" and noting that "we have no downward accountability" (Interview 4). The same interview raised concern about third-party companies associated with foreign governments and intelligence gathering: "[a UN agency] shared with Palestinian NGOs that a US based AI company, known for work with Israeli military is trying to provide them with services… we rejected… we don't have local servers, and our ownership of our data is very little, we don't know… on what clouds" (Interview 4). Cloud location, server ownership, and vendor involvement were thus understood not as neutral infrastructure choices, but as questions of sovereignty and exposure.

Similar concerns emerged in protection-oriented work. One participant explained that organizations may wish to prohibit AI use with sensitive materials but cannot fully control what staff upload: "many times there are sensitive material… we want to prohibit using AI… but you cannot guarantee that the staff will not upload this info" (Interview 7). Another warned that informal AI use carries "serious risks because sensitive personal data are uploaded into systems that may reuse or recycle the data for training and learning purposes" (Interview 5). At the same time, another interviewee captured the normalization of surveillance under siege in a stark way: "Israelis are watching us and monitoring us all the time, how is ChatGPT worse than that?" (Interview 10). Risk therefore emerged not only from misuse, but from structural lack of sovereignty over data flows in a highly securitized environment (Interviews 4, 5, 7, 10).

These risks were inseparable from labor displacement. Across the interviews, AI and digital systems were described as shifting work rather than reducing it. A MEAL practitioner noted that local partners collect field data while cleanup and formatting remain centralized: "I work with local partners who collect data in the field… I usually do data cleaning after my

partners" (Interview 3). The same participant observed that AI could take "longer time… more than traditional methods of data collection" (Interview 3). A Gaza-based practitioner described donor-imposed KoBo use as a daily burden under weak connectivity: "Our donor gave us this mobile program… KoBo… it means I will have to use it daily… we are offline a lot… language… it gets frozen… requires connectivity. I register information on papers and then use Kobo as I can" (Interview 8). Another interviewee described continuous reporting obligations: "we provide… all the data, on daily basis sometimes… activities, locations, services delivered" (Interview 10). Rather than reducing work, digital systems often generated duplicate entry, repeated formatting, constant reporting, and added verification burdens, especially under unstable connectivity.

This was especially visible in reporting requirements that demanded photographic evidence under distress. One Gaza-based worker described this as ethically violating: "I am required to take photos of activities and upload them into platforms… women feel embarrassed… if I feel really uneasy and strongly disagree with something, I will not do it" (Interview 8). What appears institutionally as documentation can function on the ground as exposure, shame, or ethical compromise.

These burdens were intensified by siege infrastructure. Electricity cuts, unstable internet, displacement, and charging difficulties were not background conditions but constitutive ones. One participant named "intermittent electricity" and cost as barriers (Interview 1). Another described the basic impossibility of stable access outside the office: "We barely have internet in Gaza… I barely get internet in my tent… its very difficult to keep mobiles and laptops charged" (Interview 8). The same interviewee could use ChatGPT "if I am in the office, but only a few times" (Interview 8). Another participant stated directly that "Data collection and assessment were severely disrupted by unstable internet connectivity" (Interview 5). The result is a stratified technological environment in which those with stable connectivity may gain some productivity advantages, while those in displacement absorb the costs of compliance without receiving the promised efficiencies.

4. Gendered Burdens, Local Voice, and Everyday Negotiation

The fourth finding is that AI-related and digital governance is lived through gendered labor, epistemic asymmetry, and everyday negotiation rather than simple compliance. Women interviewees described the collision between digital demands, care work, household survival, and ethical discomfort around documentation. One humanitarian worker linked aspirations to learn AI with the desire to increase income, then immediately negated that possibility through war and care: "I wish I had more time to learn how to use AI to increase my income, but… I need to take care… house duties… my children are always scared and always need a lot of care. I don't have time for AI" (Interview 10). AI capacity thus appears not simply as a question of training or institutional willingness, but of gendered time poverty under siege.

The same dynamic appeared in documentation practices. One interviewee described donor demands for photographs as deeply misaligned with dignity: "women feel embarrassed… children and women should be photographed in nice clothes and when they are happy" (Interview 8). She then framed the

wider system as disconnected from lived reality: "Our donors and partners outside of Gaza are losing touch with our reality, do they know that I live in a ten? Do they know that I only have one coat left to wear?" (Interview 8). In protection-oriented work, gendered risk also appeared in relation to sensitive materials and the impossibility of guaranteeing non-disclosure: "we work on… sensitive material… we want to prohibit using AI… but you cannot guarantee" (Interview 7). Digital governance is thus lived not only as technical procedure but as care labor, emotional labor, and dignity conflict under gendered conditions of responsibility and exposure (Interviews 7, 8, 10).

A related pattern concerns loss of local voice. Several interviews described AI as threatening institutional identity and local specificity when outputs became generic or donor-like. One finance manager recounted a concrete consequence: "I lost a grant… due to excessive use of AI in writing proposals… the proposal stops representing our identity and collective work… the local aspect… was wiped out… but it isn't something you can prove" (Interview 7). Another interviewee framed the issue as one of knowledge sovereignty: "Palestinian ownership of their data and protecting it… we need… [to protect] the authentic knowledge that we invested too many years in building" (Interview 4). A further participant argued for "locally owned digital infrastructure" as a condition for "meaningful digital independence" (Interview 5). Together, these accounts suggest that AI-generated outputs can flatten local specificity, institutional voice, and context-sensitive knowledge (Interviews 4, 5, 7).

At the same time, the interviews do not present staff as passive recipients of technological governance. Participants described forms of boundary work, refusal, and selective non-compliance. One local NGO practitioner advocated prohibition rather than managed adoption: "That should be prohibited. Completely" (Interview 4). The same interview described rejection of an external AI-linked service offer on political and security grounds: "Palantir AI… we rejected" (Interview 4). Another participant framed refusal as practical and embodied rather than ideological: "if I feel really uneasy and strongly disagree with something, I will not do it" (Interview 8). At the INGO level, boundary work could also appear through procedural language around digital rights and data protection, even where unofficial use continued in parallel (Interview 3). These actions do not amount to full institutional control, but they show that humanitarian AI in practice is also shaped by dispersed ethical judgment under unequal conditions.

DISCUSSION: AI, GOVERNANCE, AND POWER IN GAZA'S HUMANITARIAN SYSTEM

In Gaza-related humanitarian operations, AI functions less as innovation than as a governance mechanism that reorganizes legibility, labor, and authority under colonial constraint. The findings answer the paper's three questions in linked ways. First, staff encounter AI-related and digital systems mainly as everyday governance infrastructures embedded in administrative routines, platform dependencies, and crisis coping. Second, these systems shape coordination, decision-making, and assistance delivery through classification architectures, verification chains, reporting regimes, and platform-centered workflows that concentrate authority upward while displacing labor and risk downward. Third, frontline actors interpret, negotiate, and sometimes contest these systems through selective use, ethical boundary-setting, refusal, and survival-based adaptation under siege and institutional asymmetry. What emerges is a fragmented assemblage through which humanitarian authority is exercised and administrative burdens redistributed.

This shifts the analysis away from innovation narratives and toward governance. The key issue is not whether organizations formally "use AI," but how technological systems shape legibility, classification, contestability, and verification. Across the findings, governance is only partially formalized. Policies may exist around authorized tools, data protection, and responsible use, but in practice AI-related systems are often governed through partial rules, organizational silence, and uneven enforcement. This is what the findings identify as silent permission: informal workarounds expand into consequential tasks while responsibility is pushed downward. Governance operates less through transparent deliberation than through dispersed compliance, upstream authority, and opaque decision chains.

A decolonial reading shows that these dynamics unfold within a field already structured by external control over mobility, infrastructure, access, and visibility. AI in Gaza matters because it intensifies existing relations of bureaucratic and colonial governance. Local actors appear as data providers, verifiers, and operational users rather than authorities over the categories through which need is made legible. They enter information, check lists, and sustain workflows, while decision criteria, downstream interpretation, and infrastructural control remain external. This produces epistemic and infrastructural dependency: those closest to lived reality bear the burden of making it legible without authority over how it is classified, interpreted, or acted upon. This also explains why constrained contestability is central to the findings. Accountability is often translated into compliance rather than meaningful participation in decision-making. Staff are responsible for entering, cleaning, and verifying data, yet often lack visibility into how lists are produced, how thresholds are set, or how categories shape outcomes downstream. What appears as technical procedure is therefore also a distribution of authority.

A feminist political economy reading shows that these systems reorganize labor in ways obscured by the language of efficiency. Intensified data work is not merely technical, but also care, emotional, and accountability work performed under asymmetrical institutional conditions. Verification, follow-up, documentation, and repeated attempts to sustain legibility under crisis are disproportionately carried by those closest to households and communities, often by women. Gendered time poverty, dignity conflicts around documentation, and the pressure to manage household survival alongside institutional reporting show that digital compliance is lived through social reproduction as much as formal employment. AI and digital systems do not simply save time. They displace work downward and inward while rendering that labor less visible.

These burdens are inseparable from infrastructural and political conditions. Siege, displacement, unstable connectivity, and dependence on externally controlled platforms shape what technological systems can do, for whom, and at what cost. Digital governance promises speed, consistency, and legibility, yet often produces duplication, delay, formatting burdens, and ethical compromise under conditions in which legibility itself is difficult to sustain. The result is a technological order that depends on standardized outputs while operating in circumstances that continually undermine the possibility of producing them safely or accurately.

Finally, the findings complicate any reading of frontline actors as either passive recipients or empowered users of technology. Humanitarian workers interpret, negotiate, and sometimes refuse these systems in practice. They set boundaries, reject specific tools, work around harmful demands, and make ethical judgments under pressure. But this agency remains fragmented and constrained. It does not undo the broader asymmetry through which external actors retain disproportionate authority over infrastructures, categories, and evidence standards. It does show that humanitarian AI in practice is governed not only by formal policy, but also by dispersed judgment, refusal, and survival-based adaptation.

Taken together, the findings support a broader claim: in Gaza-related humanitarian operations, AI functions as a modality of governance that reorganizes legibility, labor, and responsibility under colonial constraint. It enters through fragmented pathways rather than coherent adoption, is governed more through risk and compliance than participatory authority, and is lived through verification burdens, epistemic dependency, infrastructural fragility, and uneven negotiation. This reframes AI in humanitarianism away from tool inventories and ethics checklists and toward a more political question: who defines categories, who carries the burden of making need legible, who can contest harmful classifications, and how technological authority is stabilized when those most affected remain least able to shape its terms.

CONCLUSION AND POLICY IMPLICATIONS

This paper examined how AI-related and digital systems enter, are governed within, and are lived through Gaza-related humanitarian operations under conditions of siege, surveillance, and external control. Across the evidence,

AI does not appear as a unified innovation agenda, but as two entangled regimes: informal staff use of generative tools to manage administrative pressure, and institutional digital systems that structure eligibility, verification, reporting, and the circulation of humanitarian data. In Gaza-related humanitarian operations, AI is not primarily a technological development but a governance mechanism that reorganizes legibility, labor, and authority under conditions of colonial constraint. Its significance lies not in technical novelty, but in how it intensifies classification, expands data circulation without sovereignty, and redistributes labor, risk, and responsibility across an unequal operational chain.

The paper's core contribution is to reframe AI in humanitarianism away from tool inventories and ethics checklists and toward governance in a colonized humanitarian space. The central questions are therefore not simply which tools are used, but who defines categories, who controls lists and verification logics, who can protect or contest data flows, and who bears the burden when systems fail. The findings show that accountability is frequently translated into compliance while contestability remains structurally constrained, and that these burdens are unevenly distributed across location, role, and gender. Under such conditions, AI's promise of efficiency is repeatedly offset by verification extraction, epistemic dependency, and the stabilization of external authority through the production of legible outputs.

Policy Implications

First, AI governance in Gaza-related operations should be treated as governance of classification and access, not merely safe tool use. Where AI or AI-adjacent practices shape eligibility, scoring, list formation, or recommendations, they should be governed as distributive decision functions with documented criteria, named decision owners, and clear responsibility for downstream effects. This is especially urgent where informal use expands through what this paper identifies as silent permission.

Second, accountability must include operational contestability. Local actors currently carry responsibility for data entry, verification, and workflow discipline while lacking visibility into how decisions are made downstream. Governance arrangements should therefore include practical mechanisms to query classifications, flag mismatches, correct errors, and challenge harmful criteria without reprisal. Responsibility should also be matched with authority: if Palestinian organizations and Gaza-based staff produce and verify the data, they should have defined influence over data fields, category design, reporting requirements, and interpretation of outputs.

Third, data protection should be treated as a political problem of governance under siege rather than as generic compliance. Data minimization should be the default, retention strictly bounded, and organizations should clearly map where data is stored, who can access it, and which vendors or cloud infrastructures are involved. Where biometric or identity-linked screening conditions access to assistance, the issue becomes structural rather than procedural.

Fourth, operational design should address labor displacement, infrastructural fragility, and dignity harms as governance concerns rather than

implementation side effects. The findings show that AI and digital systems often create duplication, continuous reporting, and ethically fraught documentation burdens under unstable connectivity and displacement. Systems should therefore reduce unnecessary verification and reporting demands, prioritize offline-first and low-bandwidth workflows, and remove dignity-harming evidence expectations, especially documentation practices that expose women, children, or displaced households to shame or ethical compromise.

Finally, humanitarian organizations should treat epistemic dependency and the erosion of local institutional voice as governance risks. AI-generated outputs can flatten context, standardize language, and weaken local specificity, while digital infrastructures remain externally controlled. Review standards should therefore protect contextual knowledge and institutional identity, and locally governed digital infrastructure should be treated not as a technical preference but as a condition of meaningful digital independence.

REFERENCES

- Ananny, Mike, and Kate Crawford. 2018. "Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability." New Media & Society 20 (3): 973–89. https://doi.org/10.1177/1461444816676645.
- Beduschi, Ana. 2022. "Harnessing the Potential of Artificial Intelligence for Humanitarian Action: Opportunities and Risks." International Review of the Red Cross 104 (919): 1149–69.
- Birhane, Abeba. 2020. "Algorithmic Colonization of Africa." Scripted 17 (2): 389–409.
- Braun, Virginia, and Victoria Clarke. 2006. "Using Thematic Analysis in Psychology." Qualitative Research in Psychology 3 (2): 77–101.
- Burrell, Jenna. 2016. "How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms." Big Data & Society 3 (1): 1–12. https://doi.org/10.1177/2053951715622512.
- Coppi, Giulio, Rebeca Moreno Jimenez, and Sofia Kyriazi. 2021. "Explicability of Humanitarian AI: A Matter of Principles." Journal of International Humanitarian Action 6 (1): 19. https://doi.org/10.1186/s41018-021-00096-6.
- Couldry, Nick, and Ulises A. Mejias. 2019a. The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism. Stanford, CA: Stanford University Press.
- Couldry, Nick, and Ulises A. Mejias. 2019b. "Making Data Colonialism Liveable: How Might Data's Social Order Be Regulated?" Internet Policy Review 8 (2): 1–24. https://doi.org/10.14763/2019.2.1411.
- Devidal, Pierrick. 2024. "Machine Learning and Humanitarian Forecasting." Humanitarian Data Studies Review 9 (1): 55–78.
- D'Ignazio, Catherine, and Lauren F. Klein. 2020. Data Feminism. Cambridge, MA: MIT Press.
- Donini, Antonio, and Daniel Maxwell. 2013. "From Face-to-Face to Face-to-Screen: Remote Management, Effectiveness and Accountability of Humanitarian Action in Insecure Environments." International Review of the Red Cross 95 (890): 383–413. https://doi.org/10.1017/S1816383114000265.
- Duffield, Mark. 2007. Development, Security and Unending War: Governing the World of Peoples. Cambridge: Polity.
- Eubanks, Virginia. 2018. Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. New York: St. Martin's Press.
- Feldman, Ilana. 2008. Governing Gaza: Bureaucracy, Authority, and the Work of Rule, 1917–1967. Durham, NC: Duke University Press.
- Fraser, Nancy. 2016. "Contradictions of Capital and Care." New Left Review 100 (July–August): 99–117.
- Geiss, Robin. 2021. Protection of Data in Armed Conflict. Geneva: Geneva Academy.
- GPPi. 2021. Research on the Specific Risks or Constraints Associated with Humanitarian Data Sharing with Donors. Berlin: Global Public Policy Institute.
- Grote, Tatjana. 2025. "Data Protection in Humanitarian Action: Military Personal Data Processing." EJIL: Talk!, November 11, 2025.
- Hilhorst, Dorothea. 2010. "Humanitarian Space as Arena: A Perspective on the Everyday Politics of Aid." Development and Change 41 (6): 1117–39. https://doi.org/10.1111/j.1467-7660.2010.01673.x.
- ICRC. 2021. "Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach." International Review of the Red Cross 102 (913): 463–79. https://doi.org/10.1017/S1816383120000454.

- Jacobsen, Katja Lindskov. 2015. The Politics of Humanitarian Technology: Good Intentions, Unintended Consequences and Insecurity. London: Routledge.
- Latonero, Mark. 2019. "Stop Surveillance Humanitarianism." New York Times, July 11, 2019.
- Madianou, Mirca. 2019. "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises." Social Media + Society 5 (3): 1–13. https://doi.org/10.1177/2056305119863146.
- Said, Edward W. 1978. Orientalism. New York: Pantheon Books.
- Scott, James C. 1985. Weapons of the Weak: Everyday Forms of Peasant Resistance. New Haven, CT: Yale University Press.
- Weitzberg, Keren, Margie Cheesman, Aaron Martin, and Emrys Schoemaker. 2021. "Between Surveillance and Recognition: Rethinking Digital Identity in Aid." Big Data & Society 8 (1): 1–7. https://doi.org/10.1177/20539517211006744.
- Wolfe, Patrick. 2006. "Settler Colonialism and the Elimination of the Native." Journal of Genocide Research 8 (4): 387–409. https://doi.org/10.1080/14623520601056240.

الهيـــمنة الرقمـــية

جامعة بيرزيت
BIRZEIT UNIVERSITY
معهد ابراهيم أبو لغد للدراسات الدولية
Ibrahim Abu-Lughod Institute of International Studies

حملة - المركز العربي
لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for
the Advancement of Social Media

ialiis@birzeit.edu
ialiis.birzeit.edu

info@7amleh.org
www.7amleh.org

UpScrolled