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

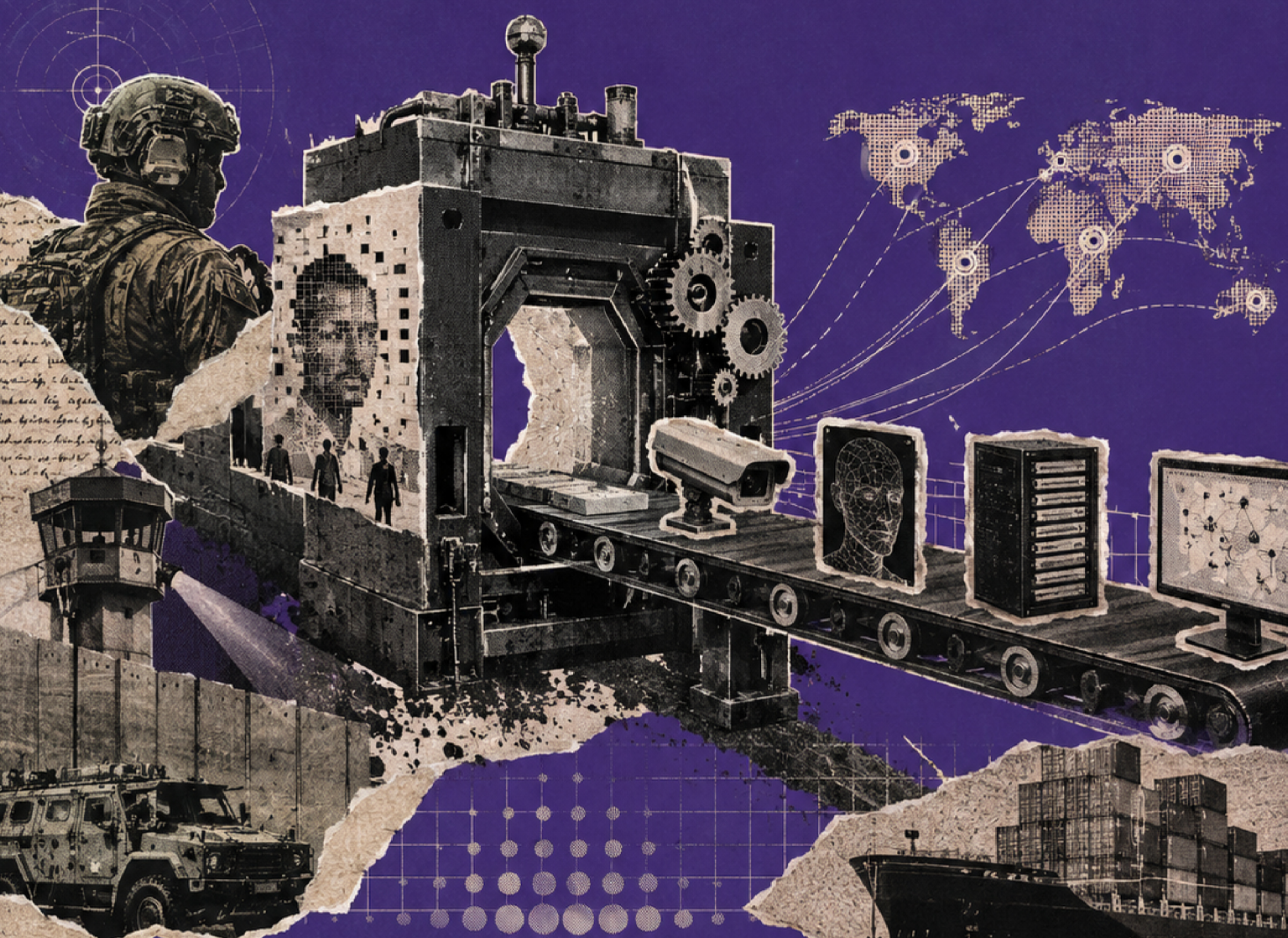
جامعة بيرزيت
BIRZEIT UNIVERSITY
معهد ابراهيم أبو لغد للدراسات الدولية
Ibrahim Abu-Lughod Institute of International Studies

Militarized Industrial Policy and Israeli Surveillance Firms

A research paper featured in the book

"Digital Domination: AI, Surveillance, and Digital Power in Palestine and Beyond"

Islam Al-Khatib



MILITARIZED INDUSTRIAL POLICY AND ISRAELI SURVEILLANCE FIRMS

ISLAM AL-KHATIB

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 "cybersecurity" 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

Contact us:

info@7amleh.org | www.7amleh.org

Our social media pages: 7amleh