



OCTOBER 13-14, 2026

Il mercato tecnologico del genocidio

*Dall'ecosistema militare israeliano alle
infrastrutture pubbliche italiane*

A cura di BDS Roma





Dati aggiornati al 27 settembre 2026

A cura di BDS Roma

Sommario

- 1** — Introduzione
- 2** — Un evento nato dentro la strategia nazionale israeliana
- 3** — Occupazione, apartheid e genocidio come questione infrastrutturale
- 4** — Dalle unità militari alle imprese e start up presenti a Roma
- 5** — Le multinazionali che sostengono l'infrastruttura
- 6** — L'ombra di Palantir
- 7** — Leonardo e Cybertech
- 8** — PSN, dati pubblici e rischio di israelizzazione della cybersecurity italiana
- 9** — Contestare Cybertech e interrompere le complicità





Introduzione

Cybertech Europe è una fiera e conferenza internazionale dedicata alla sicurezza informatica, cioè alle tecnologie e ai servizi utilizzati per proteggere reti, sistemi e dati digitali. L'edizione 2026 si svolge il 13 e 14 ottobre al centro congressi La Nuvola, nel quartiere EUR di Roma. Riunisce grandi aziende, startup, rappresentanti delle istituzioni e responsabili della sicurezza informatica. Le imprese presentano i propri prodotti, incontrano potenziali clienti e cercano collaborazioni commerciali e di ricerca. [1, 2]

Questo dossier esamina i rapporti tra Cybertech, le aziende partecipanti e l'apparato militare e tecnologico israeliano.

La manifestazione appartiene a un circuito nato in Israele, nel contesto dello sviluppo della sua industria della sicurezza informatica. Una parte di questa industria si è sviluppata attraverso il passaggio di personale, conoscenze e tecnologie dagli apparati militari e di intelligence alle imprese private.



Il dossier ricostruisce questo rapporto e analizza le forniture e le collaborazioni che collegano alcune aziende presenti alla fiera al sistema di occupazione, apartheid e genocidio contro il popolo palestinese.

L'indagine riguarda anche il coinvolgimento di realtà italiane come Leonardo. Leonardo è un gruppo industriale attivo negli armamenti, nell'aerospazio e nella sicurezza informatica, con un ruolo nella storia delle edizioni europee di Cybertech. È inoltre socio e fornitore di servizi di sicurezza del Polo Strategico Nazionale (PSN), la società che realizza e gestisce un'infrastruttura destinata a ospitare dati e servizi delle pubbliche amministrazioni italiane. L'amministratore delegato di PSN, Emanuele Iannetti, è annunciato fra i relatori dell'edizione 2026. Questa partecipazione rende necessario interrogarsi sulle aziende e sulle tecnologie alle quali vengono affidati servizi pubblici e informazioni della cittadinanza. [2-12]



Un evento nato dentro la strategia nazionale israeliana

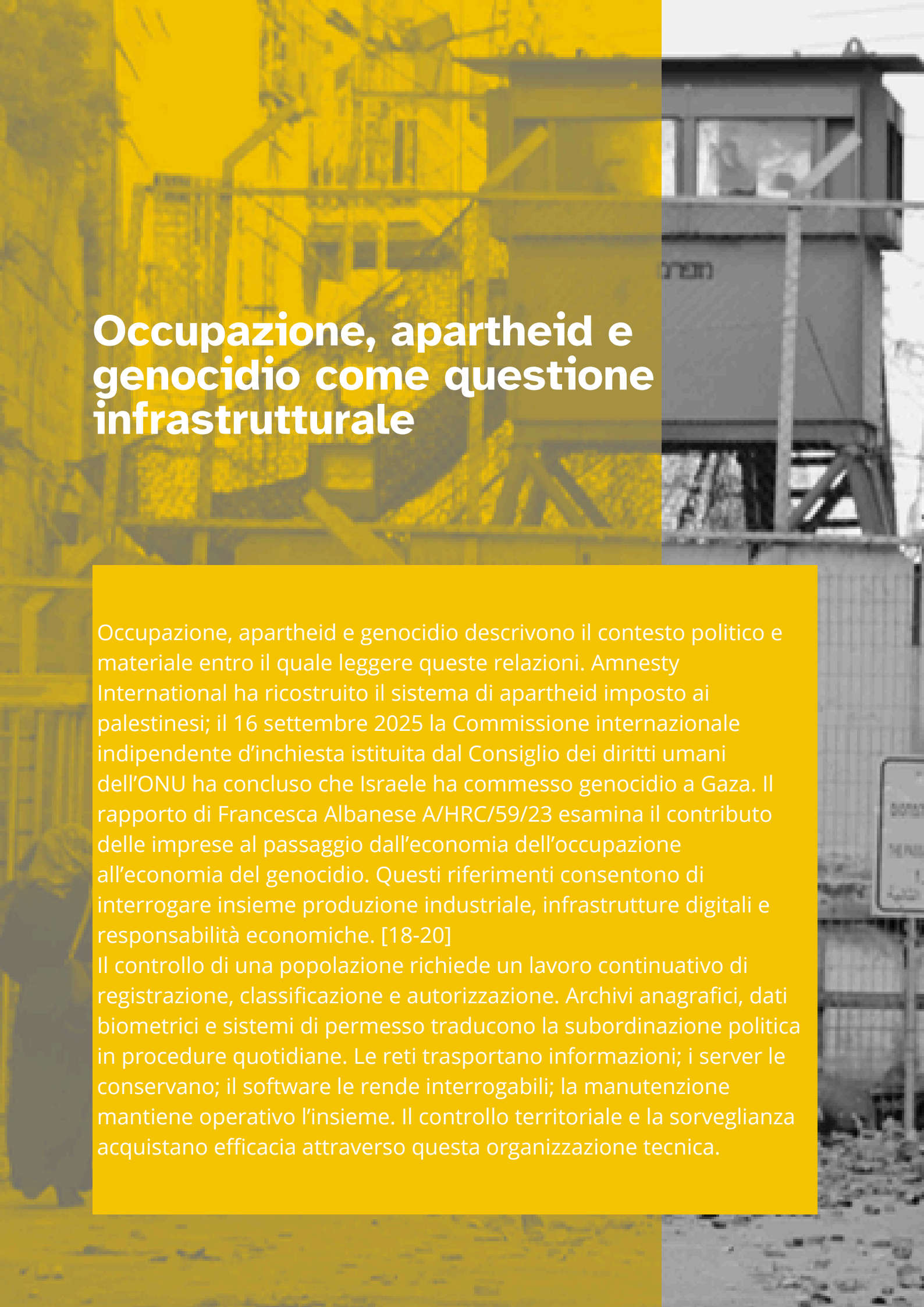
L'origine di Cybertech è documentata da fonti dei suoi stessi promotori. Il 13 gennaio 2014, il centro cyber dell'Università Ben-Gurion pubblicava l'invito alla prima conferenza, prevista a Tel Aviv il 27 e 28 gennaio. L'iniziativa era presentata da Israel Defense, dal National Cyber Bureau dell'ufficio del primo ministro, da Kenes Exhibitions e dall'università. L'apertura era affidata a Benjamin Netanyahu. Il programma mirava a riunire multinazionali, startup, investitori e clienti: la costruzione del mercato faceva parte del progetto sin dall'inizio. [13] Durante quella conferenza Netanyahu e la presidente dell'Università Ben-Gurion, Rivka Carmi, annunciarono CyberSpark, il complesso cyber di Beer-Sheva. La comunicazione dell'università descriveva la concentrazione di ricerca accademica, imprese, incubatori e agenzie pubbliche e di sicurezza.



Il disegno consisteva nel mettere in comune infrastrutture, personale qualificato e finanziamenti, trasformando la prossimità fra apparati pubblici e imprese in un vantaggio competitivo internazionale. [14]

Il fondatore di Cybertech, Amir Rapaport, è anche fondatore ed editore di IsraelDefense. Questa continuità organizzativa resta visibile nell'edizione europea 2026: il modulo per gli espositori richiama le comunicazioni del gruppo Cybertech e di IsraelDefense, mentre l'informativa privacy menziona, tra le società del gruppo Cybertech, anche Arrowmedia Israel Ltd., con sede in Israele: un elemento che documenta il collegamento societario della manifestazione con Israele. L'evento europeo si inserisce dunque in una rete editoriale e commerciale legata alla promozione dell'industria israeliana della sicurezza. [15-17]

Il problema dell'origine emerge da questa configurazione concreta. Cybertech ha contribuito alla presentazione internazionale di una strategia nazionale nella quale sviluppo economico, sicurezza e capacità militari sono strettamente collegati. Portare tale circuito a Roma permette alle sue imprese di incontrare amministrazioni e clienti europei in un contesto di riconoscimento istituzionale. La reputazione acquisita nella fiera può accompagnare l'accesso a gare, sperimentazioni e accordi di ricerca.



Occupazione, apartheid e genocidio come questione infrastrutturale

Occupazione, apartheid e genocidio descrivono il contesto politico e materiale entro il quale leggere queste relazioni. Amnesty International ha ricostruito il sistema di apartheid imposto ai palestinesi; il 16 settembre 2025 la Commissione internazionale indipendente d'inchiesta istituita dal Consiglio dei diritti umani dell'ONU ha concluso che Israele ha commesso genocidio a Gaza. Il rapporto di Francesca Albanese A/HRC/59/23 esamina il contributo delle imprese al passaggio dall'economia dell'occupazione all'economia del genocidio. Questi riferimenti consentono di interrogare insieme produzione industriale, infrastrutture digitali e responsabilità economiche. [18-20]

Il controllo di una popolazione richiede un lavoro continuativo di registrazione, classificazione e autorizzazione. Archivi anagrafici, dati biometrici e sistemi di permesso traducono la subordinazione politica in procedure quotidiane. Le reti trasportano informazioni; i server le conservano; il software le rende interrogabili; la manutenzione mantiene operativo l'insieme. Il controllo territoriale e la sorveglianza acquistano efficacia attraverso questa organizzazione tecnica.



Per questo l'analisi delle complicità deve comprendere anche attività presentate come infrastrutturali o difensive.

Amnesty ha documentato l'utilizzo nei checkpoint del sistema integrato (hardware e software) Red Wolf nel controllo biometrico dei palestinesi. Le inchieste di +972 Magazine e Local Call su Lavender e The Gospel, sistemi basati sull'intelligenza artificiale, descrivono il ruolo dell'elaborazione automatizzata delle informazioni nell'identificazione di persone e nella produzione di obiettivi umani. La rilevanza di questi casi consiste nella capacità del digitale di rendere più estesi e rapidi processi di sorveglianza e decisione con conseguenze letali. Nel genocidio a Gaza, capacità di calcolo, archiviazione e analisi diventano parte delle condizioni materiali dell'azione militare. [21-23]

La circolazione fra militare e civile ha diverse forme. Le unità tecnologiche formano personale, organizzano ricerca e sviluppano risposte a problemi operativi; imprese e fondi selezionano quelle competenze, le finanziano e le collocano sul mercato. In senso inverso, le tecnologie commerciali tornano verso apparati pubblici e militari attraverso commesse, cloud e servizi. Le acquisizioni da parte di multinazionali ampliano la disponibilità di capitali e la distribuzione internazionale. È un circuito economico, professionale e istituzionale che va esaminato nel suo insieme e che produce una dimensione di complicità strutturale.



Dalle unità militari alle imprese e start up presenti a Roma

Questa sezione raccoglie l'elenco delle aziende israeliane presenti a Cybertech Europe 2026 ed evidenzia la loro internità all'ecosistema che consente ad Israele di mantenere un sistema di apartheid, occupazione e genocidio (Tabella 1).

TABELLA 1. Aziende e startup israeliane, relazioni con l'apparato militare

Legenda: D = fornitura o collaborazione diretta documentata; I = relazione indiretta societaria o commerciale; E = appartenenza documentata all'ecosistema militare-privato attraverso personale, ricerca o finanziamento. ND = collegamento allo specifico sistema non documentato nelle fonti consultate; non significa esclusione del collegamento.

Azienda e presenza a Cybertech 2026	Relazioni documentate	Rilevanza per l'apparato militare e del controllo	Red Wolf, Gospel, Lavender e altri sistemi specifici
Check Point - espositore	D/E. Partecipazione al consorzio IC3 guidato da Israel Aerospace Industries , documentata nel 2017 e nel 2022. Il CEO Nadav Zafrir proviene dalla direzione dell'Unità 8200.	Cooperazione industriale con un gruppo militare israeliano per vendere capacità cyber a governi esteri. È un rapporto industriale concreto, oltre alla circolazione dei dirigenti fra intelligence e impresa.	ND per tutti e tre. IC3 documenta collaborazione industriale, ma non identifica i fornitori di questi sistemi. [24]
Aryon Security - startup	E. Il comunicato di lancio di Aryon collega la nascita dell'azienda all'esperienza dei fondatori in Matzov, unità di sicurezza informatica delle forze armate israeliane, e al lavoro del responsabile tecnologico nella protezione del cloud militare nell'ambito di Nimbus, il progetto cloud fornito da Google e Amazon allo Stato israeliano.	Caso esplicito di trasformazione dell'esperienza nella sicurezza del cloud militare in un prodotto commerciale.	Nimbus: collegamento professionale e tecnologico documentato. Red Wolf/Gospel/Lavender: ND. L'attività precedente dei fondatori va distinta da un contratto della startup. [25]
Gin Security - startup	E. La presentazione ufficiale richiama fondatori provenienti da Talpiot (programma di formazione militare e universitaria) e Matzov (unità delle forze armate israeliane specializzata nella crittografia e nella sicurezza informatica), premiati con l'Israel Defense Prize.	La formazione e la ricerca militari sono presentate come risorse alla base dell'impresa.	ND. La scheda identifica provenienza e competenze, non una partecipazione ai sistemi nominati. [1].
Claroty - espositore	E. Creata con il sostegno del gruppo israeliano Team8 , che fonda e finanzia imprese tecnologiche; Nadav Zafrir, ex comandante dell'Unità 8200 e già presidente di Claroty, contribuì a reclutare il gruppo di ricerca dell'azienda tra specialisti provenienti dagli apparati informatici militari israeliani.	Trasferimento organizzato di ricercatori e competenze militari verso la protezione delle infrastrutture industriali.	ND. Il nesso verificato riguarda la formazione dell'impresa e del suo gruppo di ricerca. [26]

TABELLA 1. Aziende e startup israeliane, relazioni con l'apparato militare

Azienda e presenza a Cybertech 2026	Relazioni documentate	Rilevanza per l'apparato militare e del controllo	Red Wolf, Gospel, Lavender e altri sistemi specifici
SentinelOne - espositore	E. Nel prospetto depositato nel 2021 presso la Securities and Exchange Commission (SEC), SentinelOne dichiara che il proprio personale in Israele comprende specialisti provenienti dalla cybersecurity militare e dall'intelligence israeliana.	Documenta il ruolo strutturale del personale formato nell'apparato militare nella produzione tecnologica privata.	ND. [27].
Armis - espositore; parte di ServiceNow	E/I. Percorsi militari dei fondatori; l'azienda è stata acquisita da ServiceNow nel 2026.	Integra una società nata nell'ecosistema tecnologico israeliano in una multinazionale fornitrice di amministrazioni e grandi imprese.	ND. [28]; [29].
Cynet - espositore; Marco Lucchina fra i relatori	E. La biografia del CTO Aviad Hasnis riporta nove anni nell'intelligence delle IDF.	Passaggio di competenze dall'intelligence militare alla cybersecurity commerciale.	ND. [30].
Memcyco - startup	E. Il percorso del cofondatore Israel Mazin comprende MAMRAM , struttura informatica militare israeliana.	Collegamento attraverso formazione e carriera imprenditoriale; l'impresa vende protezione dalle impersonificazioni digitali e dalle frodi.	ND. [31].
Terrogence - startup / espositore	D/E sul mercato dell'intelligence. Offre tecnologie a governi e apparati di sicurezza, valorizzando personale proveniente dall'intelligence militare. A Cybertech presenta CODEX e IRIS .	IRIS riguarda monitoraggio e deanonimizzazione su piattaforme di messaggistica; CODEX raccoglie informazioni tecniche su armi e ordigni.	CODEX (banca dati sulle armi e sulle tecniche di attacco) e IRIS (piattaforma per monitorare e analizzare attività su servizi di messaggistica come Telegram e WhatsApp): offerta attuale documentata. Face-Int (sistema di riconoscimento facciale): documentazione storica del 2018. Red Wolf/ Gospel/ Lavender e specifici impieghi contro palestinesi: ND nelle fonti qui raccolte. [32]; [33].



Check Point illustra il livello della cooperazione industriale. Nel 2017 Israel Aerospace Industries annunciò che il consorzio IC3, da essa guidato, avrebbe realizzato un centro cyber nazionale in America Latina. Check Point contribuiva con capacità di prevenzione delle minacce, controllo degli accessi e analisi forense. Nel 2022 IAI la elencava ancora fra i membri del consorzio, insieme, fra gli altri, a CyberArk e Cognyte. La cybersecurity commerciale entrava così in un'offerta esportata sotto la guida di un gruppo dell'industria militare israeliana. [24, 34]

Questo rapporto chiarisce come la dimensione civile possa concorrere alla competitività internazionale dell'industria militare. IC3 organizza prodotti differenti in un'offerta destinata agli Stati; IAI coordina la relazione con il cliente e beneficia dell'ampiezza tecnologica del consorzio. La partecipazione di Check Point a Cybertech acquista rilevanza in questa storia industriale. A essa si affiancano il percorso del suo amministratore delegato Nadav Zafir, già comandante dell'Unità 8200, e la presenza dell'impresa fra i partner del programma MATI per imprenditori riservisti: un canale di sostegno alla continuità economica delle persone mobilitate nelle IDF. [35, 36]

Aryon Security documenta con particolare chiarezza la trasformazione dell'esperienza militare in proposta commerciale. Il comunicato di lancio del 4 marzo 2025 presenta i fondatori come provenienti da Matzov. Collega inoltre la nascita della piattaforma aziendale per la protezione degli ambienti cloud all'esperienza di Ariel Litmanovich, responsabile tecnologico di Aryon, che aveva guidato un progetto pluriennale di sicurezza relativo a Nimbus nell'ambito delle forze armate israeliane.

La società spiega che le difficoltà incontrate nella protezione di un grande ambiente cloud hanno orientato la soluzione destinata ai clienti civili. Fra gli investitori individuali annunciati compaiono Shlomo Kramer, cofondatore di Check Point, e Maty Siman, fondatore di Checkmarx. Esperienza militare e capitale imprenditoriale si incontrano nella stessa impresa. [25]



Un ulteriore annuncio di Aryon presenta l'ingresso nel CTO Office di Aviv Sommer, che in precedenza aveva guidato un team di sicurezza cloud nell'ambito di un programma congiunto di Elbit Systems e delle forze armate israeliane (IDF). Si tratta di un percorso che attraversa industria militare, infrastruttura digitale e startup. Per una fiera frequentata da responsabili di servizi pubblici, questa provenienza è politicamente rilevante. [37]

Claroty offre un altro caso particolarmente istruttivo. Nel comunicato di lancio del 13 settembre 2016, l'impresa dichiarava di essere nata nell'ambito di Team8 e descriveva il reclutamento di ricercatori provenienti da un'unità cyber delle IDF con il contributo di Nadav Zafrir (vedi Tabella 1). Amir Zilberstein aveva diretto ricercatori e sviluppatori nelle IDF; Benny Porat aveva comandato un gruppo di ricerca cyber e guidato un progetto premiato con l'Israel Defense Award. La società collocava queste competenze nella protezione di reti industriali e infrastrutture critiche. [26]

Il caso Claroty rende osservabile un meccanismo organizzato di trasferimento: selezione di personale specializzato, costituzione di un gruppo di ricerca, finanziamento e accesso a mercati internazionali. Anche **SentinelOne**, nel prospetto depositato presso la SEC nel 2021, descriveva il proprio personale israeliano come proveniente dal bacino di esperti militari di cybersecurity e intelligence e situava principalmente in Israele la ricerca e sviluppo. Sono dichiarazioni rivolte al mercato finanziario, nelle quali il rapporto con l'apparato militare compare come risorsa produttiva. [27]

La scheda di **Gin Security** pubblicata da Cybertech richiama tre fondatori provenienti da Talpiot e Matzov e un Israel Defense Prize per attività di difesa basate sui dati.

Per **Armis**, l'American Technion Society ricostruisce il percorso militare e tecnologico dei fondatori; l'acquisizione completata da ServiceNow il 20 aprile 2026 inserisce l'impresa in un gruppo globale di software per organizzazioni pubbliche e private.



Il profilo di Aviad Hasnis, CTO di **Cynet**, riporta nove anni nell'intelligence delle IDF; quello di Israel Mazin, cofondatore di **Memcyco**, richiama la formazione in MAMRAM (unità centrale dei sistemi informatici, di elaborazione dati e delle infrastrutture tecnologiche delle Forze di Difesa Israeliane). Questi percorsi mostrano diversi canali di passaggio delle competenze verso il mercato. [1, 28-31]

Terrogeance rende particolarmente evidente la continuità fra intelligence e mercato privato. La società propone servizi rivolti ad agenzie governative, forze di polizia e organizzazioni di sicurezza. La sua presentazione a Cybertech insiste sulle competenze di esperti provenienti dall'intelligence militare e sull'analisi delle tracce disponibili negli ambienti digitali. La raccolta informativa è venduta come capacità operativa trasferibile al cliente. [1, 32, 38]

L'offerta illustrata per l'evento comprende CODEX, banca dati dedicata a sistemi d'arma e ordigni, e IRIS, destinato al monitoraggio e alla deanonimizzazione su piattaforme di messaggistica, fra cui Telegram e WhatsApp. La funzione politica di questi strumenti dipende dalla possibilità di ricondurre comunicazioni e identità digitali a persone identificabili. Chi decide quali soggetti monitorare, quali relazioni interpretare come sospette e quali informazioni conservare esercita un potere che supera la protezione tecnica di una rete. Face-Int appartiene alla storia di questa offerta. Nel 2018 l'ACLU, organizzazione statunitense per la difesa dei diritti civili, analizzò Face-Int, il sistema di riconoscimento facciale pubblicizzato da Terrogeance. Secondo la descrizione dell'azienda riportata dall'ACLU, il sistema raccoglieva immagini e informazioni dai profili online per creare una banca dati di volti da utilizzare per identificare le persone. Quel precedente documenta la valorizzazione commerciale di informazioni personali raccolte sul web. Per il 2026, i prodotti esplicitamente presentati nella scheda dell'evento sono CODEX e IRIS. La traiettoria dell'impresa collega così raccolta di immagini, identificazione e analisi delle comunicazioni digitali. [33]

Le multinazionali che sostengono l'infrastruttura

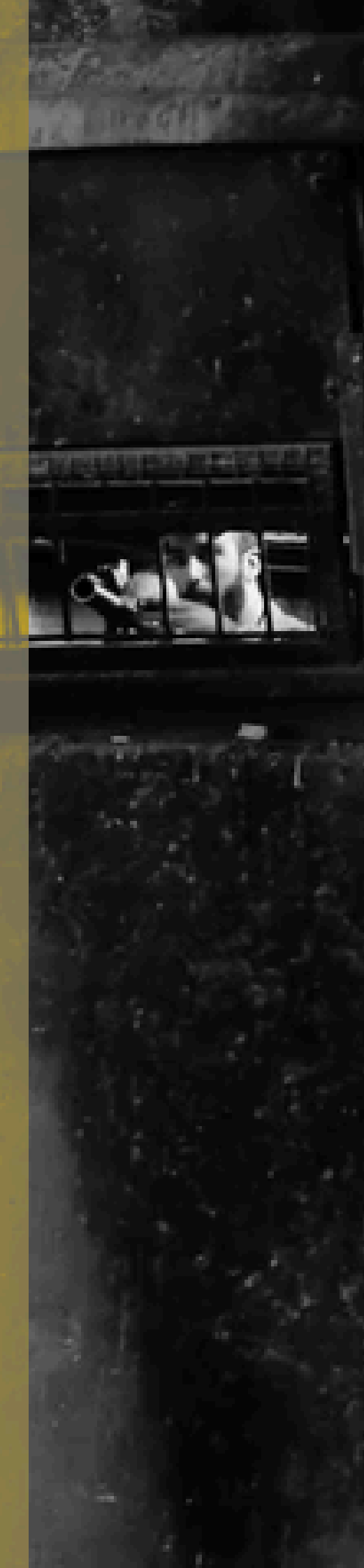


Le filiere dell'occupazione e del genocidio hanno una dimensione transnazionale.

In Tabella 2 sono raccolte le presenze non israeliane a Cybertech Europe 2026.

TABELLA 2. Multinazionali straniere e infrastrutture italiane

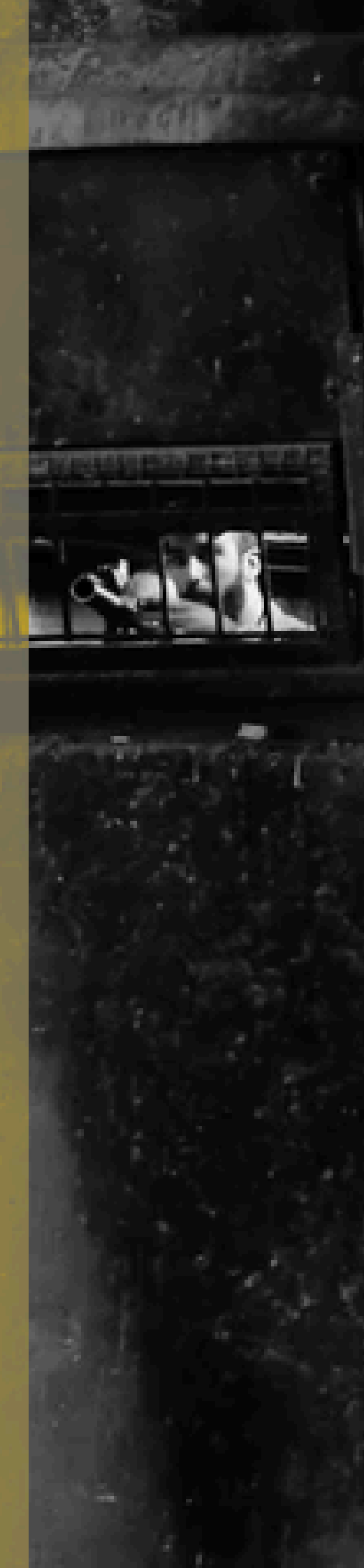
Azienda e presenza a Cybertech 2026	Relazioni documentate	Rilevanza per occupazione, apartheid e apparato militare	Red Wolf, Gospel, Lavender e altri sistemi specifici
Hewlett Packard Enterprise (HPE) - espositore; Alex Hobson relatore	D. Who Profits documenta infrastruttura biometrica (impronte digitali e immagini del volto) con estensione contrattuale fino a maggio 2028 ; server del registro Aviv , il sistema israeliano che gestisce il registro della popolazione, con contratto fino a giugno 2026; servizi alla polizia e alle carceri; nel 2024 HPE è stata selezionata per fornire l'hardware di un nuovo centro dati delle forze armate israeliane.	Aviv sostiene il registro utilizzato nel regime dei permessi palestinesi. Qui il rapporto con l'amministrazione del controllo della popolazione è specifico e documentato.	Aviv e infrastruttura biometrica: D. Basel: rapporto storico, manutenzione ereditata nel 2015, dismissione riferita a fine 2016. Passaggio Basel→Red Wolf: ND. Gospel/Lavender: ND. [39] [40].
Cisco - espositore	D. AFSC documenta server e contratti con le IDF, inclusi ordini del novembre 2023 e gennaio 2024. Who Profits ricostruisce attività negli insediamenti.	Fornitura di capacità informatiche all'apparato militare e attività economiche nell'infrastruttura dell'occupazione.	Server IDF: D. Quali server o reti sostengano Red Wolf/ Gospel/ Lavender: ND. È una domanda concreta da porre sulle destinazioni delle forniture. [41] [42].
Thales - espositore	D. Disclose ricostruisce forniture di componenti e sistemi di comunicazione a IAI ed Elbit (principale azienda privata di tecnologie per la difesa e la sicurezza di Israele), riferite a droni militari, fra 2018 e 2023.	Collegamento alla filiera materiale dei droni israeliani. Thales ha qualificato le apparecchiature di comunicazione come non letali.	Componentistica per droni: documentata dall'inchiesta. Red Wolf/Gospel/Lavender: ND. [43]
Wiz - espositore; acquisita da Google	I. Google ha completato l'acquisizione di Wiz l'11 marzo 2026. Google è, con Amazon, fornitore del progetto governativo israeliano Nimbus .	Collegamento societario a un fornitore di infrastrutture cloud utilizzabili dagli apparati pubblici e militari israeliani.	Nimbus: nesso attraverso la capogruppo. Per Wiz come fornitrice di Red Wolf/Gospel/Lavender: ND. [44]
Palo Alto Networks - espositore	I/E. Ha acquisito CyberArk l'11 febbraio 2026. CyberArk figurava nel consorzio IC3 di IAI nel 2022.	Il gruppo incorpora una società con una collaborazione documentata con l'industria militare israeliana. La fonte sul consorzio è del 2022: la continuità dell'accordo dopo l'acquisizione richiede verifica.	ND. L'acquisizione non identifica il gruppo come produttore dei sistemi nominati. [45]



HPE, Cisco e Thales, annunciate a Cybertech, occupano posizioni differenti nella disponibilità di capacità informatiche e militari. La loro presenza permette di osservare il contributo di imprese straniere alla continuità operativa degli apparati israeliani e alla loro integrazione nei mercati tecnologici globali.

Who Profits documenta le forniture di **HPE** agli enti israeliani che gestiscono il registro della popolazione, la polizia, le carceri e le infrastrutture militari: server, apparecchiature informatiche e servizi di assistenza e manutenzione. La scheda riporta un'estensione fino a maggio 2028 della fornitura per l'infrastruttura biometrica nazionale; il contratto per server e manutenzione di Aviv, il sistema informatico dell'Autorità israeliana per la popolazione e l'immigrazione che amministra anche i permessi necessari agli spostamenti dei palestinesi, arrivava a giugno 2026. Sono inoltre documentati assistenza e manutenzione dei server e delle infrastrutture informatiche del servizio penitenziario israeliano da marzo 2025 a febbraio 2026, l'intenzione annunciata dalla polizia di estendere Data Center Care (servizio di assistenza e manutenzione informatica) fino a dicembre 2026 e la selezione riferita nel luglio 2024 per un nuovo centro dati militare. [39]

Il coinvolgimento di HPE nei sistemi di controllo biometrico dei palestinesi ha un precedente in Basel, utilizzato nei checkpoint militari israeliani per verificare l'identità delle persone e controllarne il passaggio. Secondo AFSC Investigate, HPE ne ereditò la manutenzione nel 2015, dopo la divisione del gruppo Hewlett-Packard; Basel fu dismesso alla fine del 2016. Si trattava quindi di un sistema precedente a Red Wolf, con una funzione di controllo analoga, ma senza una successione tecnologica accertata tra i due.



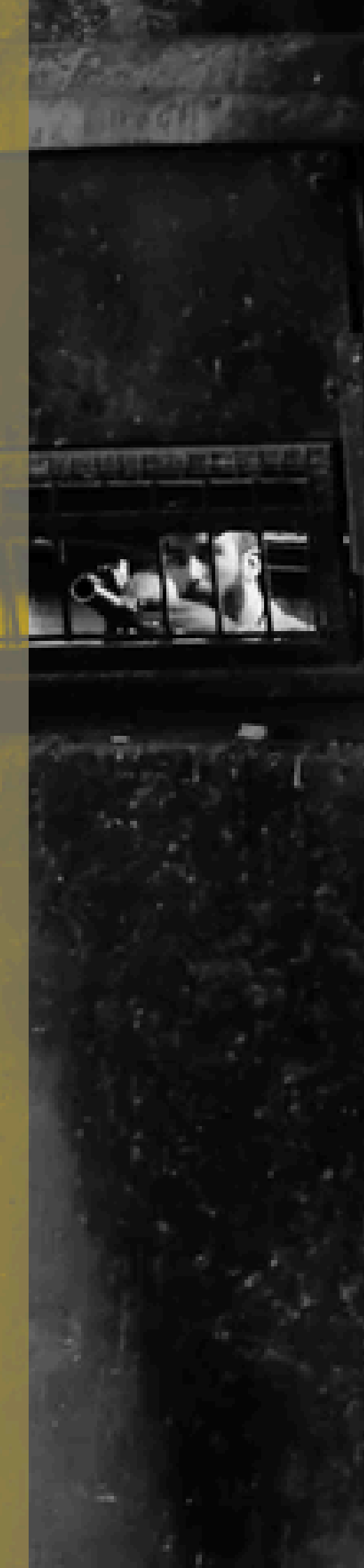
Nel 2017 la divisione dei servizi informatici di HPE si unì a CSC, formando DXC Technology.

Per ricostruire il successivo coinvolgimento di HPE occorre quindi considerare le forniture rimaste all'azienda, fra cui quelle per il registro della popolazione, le infrastrutture biometriche, la polizia e le carceri israeliane. [40, 48]

Per **Cisco**, AFSC documenta forniture di server alle forze armate israeliane (IDF), attraverso un contratto del 2017 e ulteriori commesse tra novembre 2023 e gennaio 2024. Who Profits ricostruisce inoltre attività dell'azienda negli insediamenti israeliani della Cisgiordania e del Golan occupato.

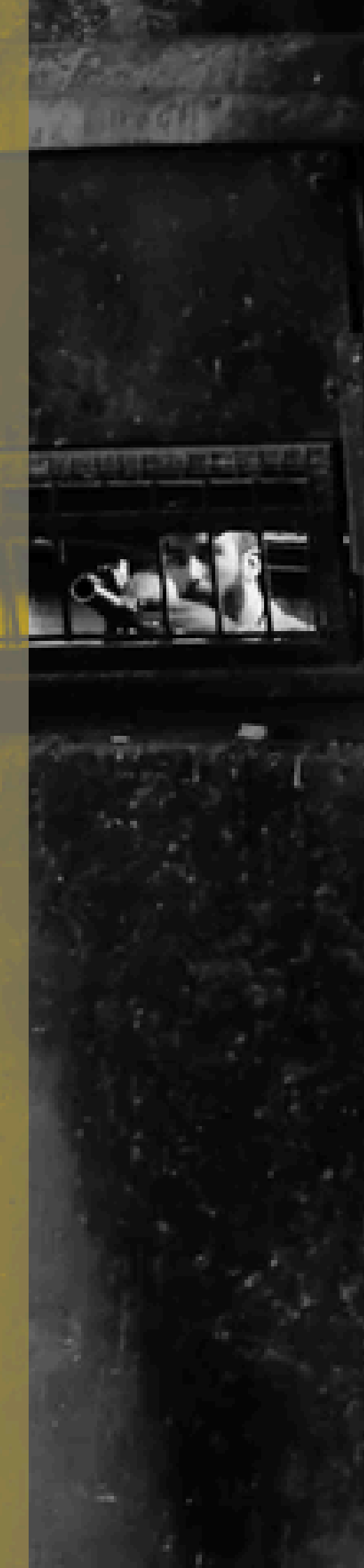
Server e reti consentono agli apparati militari di conservare ed elaborare dati, scambiare informazioni e mantenere operativi i propri sistemi informatici. Il contributo di queste forniture riguarda quindi le condizioni materiali del loro funzionamento: la disponibilità di infrastrutture affidabili permette di utilizzare le informazioni e coordinare le attività con continuità. Per questo, anche le tecnologie informatiche di uso generale devono essere considerate nell'analisi del sostegno all'apparato militare israeliano. [41, 42]

Per **Thales**, l'inchiesta di Disclose del 13 marzo 2025 ricostruisce, attraverso dodici fatture, vendite di componenti e sistemi di comunicazione a IAI ed Elbit, per circa due milioni di euro fra il 2018 e il 2023, riferite a droni militari. Thales ha confermato vendite a entità israeliane, qualificando i sistemi di comunicazione come non letali. Il loro ruolo industriale resta centrale: un velivolo dipende anche dai sistemi che consentono comunicazione e funzionamento. La filiera militare comprende questi componenti insieme alla piattaforma e all'armamento. [43]



Il progetto Nimbus, attraverso cui Google e Amazon forniscono servizi cloud allo Stato israeliano, comprende anche il Ministero della Difesa e le forze armate. Queste infrastrutture permettono di archiviare ed elaborare grandi quantità di dati, ampliando le capacità degli apparati che le utilizzano. **Wiz**, presente a Cybertech e acquistata da Google nel marzo 2026, appartiene allo stesso gruppo che fornisce queste infrastrutture. La rilevanza della sua presenza riguarda quindi anche la proprietà aziendale: acquistare servizi Wiz significa sostenere economicamente una società del gruppo Google, coinvolto nelle forniture cloud agli apparati israeliani. [44, 49, 50]

Palo Alto Networks aggiunge un'altra forma di integrazione. L'11 febbraio 2026 ha completato l'acquisizione di CyberArk, elencata da IAI nel consorzio IC3 nel 2022. La ricostruzione mette in relazione il gruppo attuale con una collaborazione industriale documentata della società acquisita. Le acquisizioni incorporano imprese, personale e posizioni di mercato; per comprenderne le conseguenze politiche occorre seguire anche la storia industriale delle controllate. [24, 45]



L'ombra di Palantir

Palantir è una società statunitense e il suo rapporto con Israele è contrattuale e politico. Nel gennaio 2024 annunciò un accordo strategico con il Ministero della Difesa israeliano. Il rapporto Albanese ne analizza il ruolo nell'apparato militare.

Palantir non risulta direttamente annunciata nell'elenco degli espositori o dei relatori consultato. La sua rilevanza per Cybertech consiste nella rete commerciale documentata con Cloudflare, Cisco e Accenture, tutte presenti nell'elenco 2026. Per ricostruire i legami di Cybertech con Palantir, non basta verificare se quest'ultima abbia uno stand: occorre esaminare anche i rapporti commerciali e tecnologici che intrattiene con aziende presenti alla fiera, come Cloudflare, Cisco e Accenture. Questi rapporti collegano Palantir a imprese partecipanti, senza equivalere a una sua partecipazione all'evento. [20, 51]

Cloudflare è collegata a Palantir da una partnership resa pubblica nel 2023 per l'ottimizzazione dei costi cloud.



Cisco ha due tipi di rapporto con Palantir. È già cliente di Apollo, il software di Palantir che permette di installare, aggiornare e gestire programmi su diverse infrastrutture informatiche. Il 10 settembre 2026 ha inoltre annunciato una collaborazione per offrire soluzioni che combinano le tecnologie delle due aziende.

In questa collaborazione, Cisco mette a disposizione l'infrastruttura informatica, sviluppata con NVIDIA e chiamata Secure AI Factory: server, reti e sistemi necessari a far funzionare applicazioni di intelligenza artificiale. Palantir fornisce il software: Sovereign AI OS, per utilizzare dati e intelligenza artificiale mantenendone il controllo nell'ambiente scelto dal cliente, e Ontology for Cybersecurity, che collega informazioni su dispositivi, utenti, sistemi e minacce per supportare le attività di sicurezza informatica.

Il risultato è un'offerta congiunta: i clienti possono adottare software Palantir attraverso una soluzione costruita sull'infrastruttura Cisco e NVIDIA. È in questo senso che la collaborazione amplia i canali commerciali attraverso cui Palantir può raggiungere nuovi clienti.

[47, 52, 53]

Accenture rende questa rete ancora più estesa. Il 16 dicembre 2025 le due società hanno annunciato l'Accenture Palantir Business Group e la designazione di Accenture come partner globale preferenziale. Nel 2026 Accenture ha descritto l'integrazione delle proprie capacità cyber con Palantir Apollo per individuare vulnerabilità, automatizzare la distribuzione del software e gestire aggiornamenti in ambienti cloud, locali e isolati. [46, 54]



Leonardo e Cybertech

Leonardo ha avuto un ruolo importante nelle precedenti edizioni europee di Cybertech: la brochure del 2023 indicava che l'evento era realizzato in collaborazione con l'azienda; nel 2024 Leonardo annunciava sul proprio sito la partecipazione del gruppo e dei suoi massimi dirigenti. Le fonti del 2025 mostrano una visibilità diversa rispetto alle edizioni precedenti. Per il 2026, il collegamento più chiaramente documentato passa dalla presenza del CEO del Polo Strategico Nazionale (PSN), società partecipata da Leonardo e destinataria del suo contributo operativo alla cybersecurity. [5-10]

Il gruppo che ha contribuito alla promozione della fiera è anche fornitore militare di Israele e socio di un'infrastruttura strategica per la PA italiana. La minore visibilità del marchio non esaurisce la questione della sua influenza: il punto è il ruolo nei servizi, nella governance e nelle relazioni con i fornitori.

Le risposte agli azionisti del maggio 2026 offrono un riscontro diretto sulle forniture a Israele.



Leonardo riconosce contratti ancora in esecuzione per materiali e servizi relativi agli M-346. Dichiara inoltre un contratto del 2019 con il Ministero della Difesa israeliano per complessi navali 76/62 e spedizioni di ricambi e attrezzature, dopo il 7 ottobre 2023 e fino al 2024, per circa 465.000 euro. L'azienda richiama licenze rilasciate prima della sospensione delle nuove autorizzazioni. [3, risposte 2.8-2.11]

Il rapporto industriale con Israele comprende inoltre l'incorporazione di RADA, produttrice israeliana di radar tattici, attraverso la fusione completata da Leonardo DRS nel novembre 2022. Il legame attraversa quindi tanto la fornitura quanto l'integrazione societaria. [55]

Due espositori presenti a Cybertech 2026 sono interlocutori industriali documentati di Leonardo. Con Cisco il memorandum del 13 aprile 2023 prevedeva cooperazione civile e nella difesa, opportunità commerciali congiunte e gruppi di lavoro su cybersecurity, reti sicure e cloud edge (modello tecnologico che porta le risorse del cloud computing direttamente ai margini della rete, cioè il più vicino possibile ai dispositivi e agli utenti che generano e utilizzano i dati). Fra gli ambiti prospettati figuravano droni e sistemi avanzati di sicurezza urbana. Con Thales, Leonardo condivide Telespazio, partecipata rispettivamente al 67% e al 33%, e Thales Alenia Space, con quote inverse. Questi rapporti collocano la fiera dentro una rete industriale già organizzata. [56, 57]

Il nodo Cisco è particolarmente significativo: collega forniture alle IDF, cooperazione con Leonardo e collaborazione con Palantir. La rete si ricostruisce attraverso accordi distinti, ciascuno con propri oggetti e destinatari. Politicamente, la convergenza mostra come infrastrutture (CISCO), industria militare (Leonardo) e software di analisi (Palantir) possano rafforzare reciprocamente la propria presenza sul mercato della sicurezza.





PSN, dati pubblici e rischio di israelizzazione della cybersecurity italiana

Il Polo Strategico Nazionale (PSN) nasce per ospitare dati e servizi della pubblica amministrazione. La sua presenza a Cybertech, attraverso il CEO Emanuele Iannetti, annunciato fra i relatori del 2026, porta quindi nella fiera un soggetto le cui scelte incidono sulla continuità dei servizi pubblici, sulla tutela delle informazioni personali e sull'autonomia tecnologica delle amministrazioni. Partecipare a uno spazio commerciale che promuove anche imprese legate all'apparato militare e di intelligence israeliano significa offrire loro riconoscimento istituzionale e occasioni di accesso al mercato pubblico italiano. È questa funzione che rende la partecipazione di PSN politicamente contestabile. [2]

Leonardo occupa nel Polo una posizione sia societaria sia operativa. Al 25 settembre 2026, la pagina ufficiale PSN riporta TIM al 45%, Leonardo al 25%, CDP Equity al 20% e Sogei al 10%. Il riassetto annunciato va distinto dalle quote effettivamente pubblicate: Poste ha comunicato che l'accordo del 16 giugno per acquistare la partecipazione di CDP Equity è soggetto a condizioni, con completamento atteso entro fine anno; il 23 settembre CorCom ha riferito il progetto di acquisizione del 10% di Sogei da parte di Leonardo, che porterebbe quest'ultima al 35%. [4, 58, 59]



Il ruolo di Leonardo comprende inoltre prestazioni e responsabilità nella sicurezza informatica. Il manuale tecnico PSN del 21 marzo 2024 indica il gruppo fra i soggetti responsabili dei trattamenti di cybersecurity per specifici servizi, compresi servizi basati su Google. Questo contributo operativo, già richiamato nel comunicato sulla costituzione dell'infrastruttura, rende il rapporto con PSN più profondo di una semplice partecipazione finanziaria: Leonardo interviene nella protezione dei sistemi attraverso cui vengono gestiti dati pubblici. [10, 60]

Il Polo Strategico Nazionale (PSN) ospita dati e applicazioni delle amministrazioni pubbliche italiane utilizzando anche tecnologie di Google, Amazon Web Services (AWS), Microsoft e Oracle. Il funzionamento varia secondo il servizio scelto: in alcuni casi PSN gestisce direttamente sistemi riservati alle amministrazioni, con specifiche garanzie sul controllo delle chiavi digitali necessarie a rendere leggibili i dati cifrati; in altri casi utilizza i centri dati situati in Italia di queste multinazionali.

Google e Amazon sono anche i fornitori di Nimbus, il progetto cloud israeliano che comprende servizi destinati al Ministero della Difesa e alle forze armate. Le stesse aziende ricevono quindi commesse sia per la digitalizzazione della pubblica amministrazione italiana sia per le infrastrutture informatiche degli apparati israeliani. Questo è un collegamento economico e industriale da evidenziare: la scelta dei fornitori del cloud pubblico italiano sostiene anche gruppi che lavorano per quegli apparati. Non significa che i dati italiani siano condivisi con Israele.



A Cybertech è inoltre annunciata Wiz, azienda di sicurezza informatica acquistata da Google: la sua partecipazione porta alla fiera una società appartenente a uno dei gruppi coinvolti tanto nei servizi offerti da PSN quanto nel progetto Nimbus. [12, 44, 49]

È questa traiettoria che definiamo **rischio di israelizzazione della cybersecurity pubblica italiana**: l'incorporazione stabile di filiere nelle quali l'esperienza militare israeliana viene trasformata in prodotti, ricavi e prestigio professionale. Il problema riguarda la possibilità che la domanda pubblica italiana alimenti un ecosistema tecnologico intrecciato alle pratiche di controllo che sostengono l'occupazione, l'apartheid e il genocidio contro il popolo palestinese. Acquisti e partnership possono trasferire a questo ecosistema risorse economiche e legittimazione, creando al tempo stesso dipendenze difficili da sciogliere.

La dipendenza prende forma nelle scelte tecniche quotidiane: software proprietari, formati poco trasferibili, manutenzione affidata al produttore, aggiornamenti e integrazioni che rendono costoso cambiare fornitore. Avere i server in Italia non basta a garantire sovranità digitale. Occorre sapere chi controlla software e chiavi, chi può intervenire da remoto, quali subfornitori partecipano al servizio e quali attività l'amministrazione possa continuare a svolgere autonomamente. La ricerca dell'Agenzia dell'Unione europea per la cybersicurezza (ENISA) sulla sicurezza delle catene di fornitura attribuisce proprio alla gestione dei fornitori un ruolo essenziale. La protezione dei dati e la responsabilità politica per le imprese finanziate dalla spesa pubblica devono quindi essere valutate insieme. [61]



La questione riguarda anche i dati delle studentesse e degli studenti e le aziende pagate per conservarli e proteggerli. Il dossier *La scuola di Leonardo*, curato da BDS Roma, ricostruisce il precedente ruolo di Leonardo nella gestione dei sistemi informatici del Ministero dell'Istruzione e il passaggio operativo, dal 2022, a Sogei, società informatica interamente controllata dal Ministero dell'Economia e delle Finanze. [62]

Una memoria del Ministero dell'Istruzione e del Merito, presentata alla Camera nel luglio 2025, descrive il trasferimento dei sistemi nei centri dati di Sogei e il percorso per spostare alcune applicazioni nel cloud, cioè su infrastrutture informatiche accessibili attraverso la rete. In questo percorso interviene anche il Polo Strategico Nazionale (PSN), di cui Leonardo è socio e al quale fornisce servizi di sicurezza informatica. Il documento richiama inoltre un accordo per gli acquisti informatici delle amministrazioni, denominato Sistema Pubblico di Connettività (SPC), che definisce fornitori, servizi, prezzi e condizioni. [63, 64]

Il problema politico è che la gestione dei servizi digitali pubblici può generare ricavi per Leonardo, un gruppo che fornisce anche armamenti e servizi all'apparato militare israeliano. Attraverso il suo ruolo in PSN, Leonardo partecipa all'infrastruttura destinata a custodire dati pubblici: occorre quindi chiarire quali servizi scolastici siano interessati e quali incarichi e risorse economiche spettino al gruppo.

Per ogni sistema, dall'Anagrafe degli studenti alle applicazioni utilizzate dalle scuole, bisogna sapere dove sono conservati i dati, quali aziende li gestiscono, chi può consultarli e per quali finalità.



La partecipazione azionaria di Leonardo a PSN e il suo ruolo attivo nella gestione della cybersecurity non chiariscono, da soli, quali informazioni l'azienda possa trattare: renderli conoscibili è particolarmente importante quando si tratta di **dati su minori, disabilità e percorsi scolastici**.

Per le comunità scolastiche, chiedere trasparenza significa quindi tutelare le informazioni personali e contestare la destinazione del denaro pubblico. Le risorse per la digitalizzazione dell'istruzione non devono sostenere imprese coinvolte nelle filiere dell'occupazione, dell'apartheid e del genocidio. La richiesta politica è interrompere questi rapporti, a partire dal ruolo di Leonardo nei servizi digitali pubblici, e impedire che la partecipazione di PSN a Cybertech apra ulteriori collaborazioni con aziende coinvolte.





Contestare Cybertech e interrompere le complicità

Cybertech riunisce ciò che la retorica dell'innovazione tende a separare: competenze sviluppate negli apparati militari, imprese che le trasformano in prodotti e profitti, istituzioni pubbliche che possono acquistarle e legittimarle. Le origini dell'evento, i rapporti industriali delle aziende partecipanti e la presenza di PSN rendono questi legami visibili anche a Roma.

La partecipazione di amministrazioni pubbliche e organizzazioni come Cloud Security Alliance (CSA) ed European Organisation for Security (EOS) rafforza l'autorevolezza della manifestazione e il suo accesso alle reti industriali e istituzionali. CSA vi porta il prestigio di un'organizzazione internazionale della sicurezza cloud che, nel 2022, ha sottoscritto un accordo di cooperazione con l'Israel National Cyber Directorate. EOS, rappresentante dell'industria europea della sicurezza, contribuisce al collegamento fra imprese, ricerca e decisori pubblici. Il loro sostegno è politicamente contestabile perché accredita uno spazio commerciale nel quale operano anche aziende coinvolte nelle filiere dell'occupazione, dell'apartheid e del genocidio. Chiederne il ritiro significa intervenire sui meccanismi che trasformano questi rapporti in riconoscimento professionale e opportunità economiche. [1, 2, 65]



Nella prospettiva della **campagna di BDS Italia per l'embargo militare a Israele**, contestare Cybertech significa intervenire sui rapporti economici e istituzionali che sostengono l'occupazione, l'apartheid e il genocidio: dalle forniture di armi e componenti ai servizi destinati agli apparati di controllo, dalle collaborazioni industriali agli spazi nei quali queste relazioni vengono promosse come normali occasioni di affari.

Un obiettivo prioritario è il ritiro della concessione degli spazi della Nuvola, all'EUR. La direzione e il soggetto gestore del centro congressi devono essere chiamati a rispondere pubblicamente della scelta di ospitare Cybertech, contribuendo alla sua realizzazione e visibilità. Su questa responsabilità può concentrarsi la pressione di collettivi solidali con la Palestina, reti antimilitariste, organizzazioni sindacali e realtà studentesche, attraverso richieste pubbliche, iniziative di denuncia e presidi.

A PSN e alle amministrazioni pubbliche va chiesto di ritirare la propria partecipazione alla manifestazione. Il ritiro deve accompagnarsi all'impegno a non avviare, attraverso la fiera, accordi, acquisti o sperimentazioni con le aziende coinvolte nelle filiere denunciate e a rendere pubblici eventuali rapporti già intrapresi.

Il programma di Cybertech Europe 2026 non è ancora definitivo e nuove presenze potranno ampliare i rapporti da indagare. Il quadro già disponibile offre tuttavia una base concreta per collegare inchiesta, denuncia e pressione politica.

Contestare Cybertech significa impedire che le istituzioni e le risorse pubbliche diventino strumenti di normalizzazione e sostegno dell'apparato militare e tecnologico israeliano.

Fonti e documenti

AFSC indica American Friends Service Committee; Investigate è il suo progetto di ricerca sulle imprese.

Who Profits è un centro di ricerca sull'economia dell'occupazione.

[1] Cybertech.[Sponsor espositori e startup 2026](#)

[2] Cybertech.[Relatori 2026](#)

[3] Leonardo.[Risposte preassembleari maggio 2026, quesiti 2.8-2.11, pagine 13-14](#)

[4] Polo Strategico Nazionale.[Composizione del capitale e quota Leonardo](#)

[5] Cybertech.[Brochure Europe 2023: collaborazione con Leonardo](#)

[6] Polo Strategico Nazionale.[Partecipazione a Cybertech Europe 2023, 5 ottobre 2023](#)

[7] Leonardo.[Cybertech Europe 2024: vertici e partecipazione](#)

[8] Cybertech.[Agenda Europe 2025: versione web consultata](#)

[9] ITKeyMedia.[Presentazione Cybertech Europe 2025, 16 giugno 2025](#)

[10] Leonardo.[Accordo per l'infrastruttura cloud della PA, 26 agosto 2022](#)

[11] Polo Strategico Nazionale.[Innovation Hub: ricerca, sviluppo e collaborazioni](#)

[12] Polo Strategico Nazionale.[Servizi con Cloud Service Provider e garanzie dichiarate](#)

[13] Università Ben-Gurion.[Invito alla prima Cybertech, 13 gennaio 2014](#)

[14] Americans for Ben-Gurion University.[Annuncio CyberSpark a Cybertech, 28 gennaio 2014](#)

[15] UVID Tech.[Profilo di Amir Rapaport e rapporto con IsraelDefense](#)

[16] Cybertech.[Modulo espositori e riferimento a IsraelDefense](#)

[17] Cybertech.[Privacy Notice, entità del gruppo e contitolarità](#)

[18] Commissione internazionale indipendente d'inchiesta / OHCHR.[Conclusioni sul genocidio a Gaza, 16 settembre 2025](#)

[19] Amnesty International.[Rapporto sull'apartheid, 2022](#)

[20] Francesca Albanese / OHCHR.[Rapporto A/HRC/59/23 From economy of occupation to economy of genocide, 2025](#)

[21] +972 Magazine.[Inchiesta su Lavender, 3 aprile 2024](#)

[22] Amnesty International.[Automated Apartheid, 2023](#)

[23] +972 Magazine / Local Call.[Inchiesta su Gospel e produzione automatizzata di obiettivi, 30 novembre 2023](#)

[24] Israel Aerospace Industries.[Membri IC3 e ingresso Checkmarx, 2022](#)

[25] Aryon Security.[Comunicato di lancio, 4 marzo 2025](#)

[26] Claroty.[Lancio della società e reclutamento dalle IDF, 13 settembre 2016](#)

[27] SentinelOne / SEC.[Prospetto S-1/A, 2021, sezioni Our Team e Research and Development](#)

[28] American Technion Society.[Profilo dei fondatori Armis](#)

[29] ServiceNow.[Completamento acquisizione Armis, 20 aprile 2026](#)

[30] Security Magazine.[Profilo di Aviad Hasnis, Cynet](#)

[31] Pulse 2.0.[Intervista a Israel Mazin, Memcyco](#)

[32] Terrogeance.[Offerta aziendale corrente](#)

[33] ACLU.[Analisi di Face-Int e raccolta di immagini online, 16 aprile 2018](#)

[34] Israel Aerospace Industries.[Contratto IC3 in America Latina, 27 maggio 2017](#)

[35] Check Point.[Leadership aziendale](#)

[36] MATI Jerusalem.[Programma per imprenditori riservisti e partner](#)

[37] Aryon Security.[Annuncio aziendale sull'ingresso di Aviv Sommer](#)

[38] Terrogeance.[Profilo aziendale e destinatari dei servizi](#)

- [39] Who Profits.[HPE, contratti e sistemi del controllo](#)
- [40] AFSC Investigate.[HPE e vicenda Basel](#)
- [41] AFSC Investigate.[Cisco e forniture militari](#)
- [42] Who Profits.[Cisco e attività negli insediamenti](#)
- [43] Disclose.[Inchiesta sulle forniture Thales a IAI ed Elbit, 13 marzo 2025](#)
- [44] Google.[Completamento acquisizione Wiz, 11 marzo 2026](#)
- [45] Palo Alto Networks.[Completamento acquisizione CyberArk, 11 febbraio 2026](#)
- [46] Accenture.[Accenture Palantir Business Group, 16 dicembre 2025](#)
- [47] Palantir.[Partnership con Cloudflare, 2023](#)
- [48] Who Profits.[Riorganizzazione HP HPE e DXC, agosto 2017](#)
- [49] Governo israeliano.[Project Nimbus e soggetti coinvolti](#)
- [50] +972 Magazine.[Inchiesta sui cloud commerciali e l'esercito israeliano, 4 agosto 2024](#)
- [51] CTech / Calcalist.[Accordo Palantir e Ministero della Difesa israeliano, gennaio 2024](#)
- [52] Palantir.[Apollo e clienti, incluso Cisco, 2023](#)
- [53] Cisco.[Collaborazione con Palantir per IA e cybersecurity, 10 settembre 2026](#)
- [54] Accenture.[Collaborazione con Palantir Apollo nella cybersecurity, 2026](#)
- [55] Leonardo DRS.[Completamento fusione con RADA, 28 novembre 2022](#)
- [56] Thales Alenia Space.[Space Alliance e quote delle joint venture con Leonardo](#)
- [57] Leonardo.[Memorandum di cooperazione con Cisco, 13 aprile 2023](#)
- [58] Poste Italiane.[Risultati semestrali, 24 luglio 2026: acquisto quota PSN soggetto a condizioni, p. 23](#)
- [59] CorCom.[Riassetto PSN prospettato: Poste e Leonardo, 23 settembre 2026](#)
- [60] Polo Strategico Nazionale.[Manuale tecnico misure di sicurezza, 21 marzo 2024, ed. 1 v. 02, pp. 31-35](#)
- [61] ENISA.[Good Practices for Supply Chain Cybersecurity, 2023](#)
- [62] BDS Roma, [La scuola di Leonardo](#)
- [63] Ministero dell'Istruzione e del Merito / Camera dei deputati.[Memoria acquisita il 23 luglio 2025: infrastrutture Sogei e PSN, pp. 4 e 13-14](#)
- [64] BDS Roma.[La scuola di Leonardo, giugno 2026, cap. 9 pp. 51-54. Presentazione e accesso al dossier](#)
- [65] Cloud Security Alliance.[Memorandum con Israel National Cyber Directorate, 27 ottobre 2022](#)