LES PORTES D'ENTRADA DE LA TECNOLOGIA DEL GENOCIDI A EUROPA

La traçabilitat del sector militar i de vigilància israelià al mercat europeo.

RESUM EXECUTIU

Israel ha utilitzat armament i tecnologies militars avançades —incloent eines basades en intel·ligència artificial— durant el genocidi del poble palestí. Aquesta situació, junt als atacs d'Israel i dels Estats Units al Líban i Iran, promou la transferència pràctiques de control, vigilància i repressió cap a altres contextos, inclosa Europa. A partir del mapeig d'empreses implicades i dels seus circuits de finançament, aquest informe identifica com aquestes tecnologies i actors s'integren al mercat europeu, en el marc d'una relació creixent entre la UE i Israel en matèria militar i de seguretat. La recerca analitza nou vies principals d'entrada d'aquestes empreses a Europa, posant de manifest els mecanismes polítics, econòmics i institucionals que en faciliten la penetració, i les seves implicacions en termes de drets humans i coherència amb el dret internacional.

1. El rearmament europeu a través de l'OTAN i del Pla Rearm Europe:

El rearmament europeu impulsat per l'Organització del Tractat de l'Atlàntic Nord (OTAN) i el Pla *Rearm Europe* obre un ampli mercat per a tecnologies militars i de seguretat. L'èmfasi en la innovació ràpida, interoperabilitat i producció massiva afavoreix la incorporació de sistemes desenvolupats per empreses israelianes o pels seus socis europeus. Instruments com *Defence Innovation Accelerator for the North Atlantic (Accelerador d'Innovació de Defensa per a l'Atlàntic Nord, DIANA per les seves sigles en anglès), el NATO Innovation Fund (Fons d'Innovació de l'OTAN) o la NATO Support and Procurement Agency (Agència de Suport i Contractació de l'OTAN) actuen com a acceleradors d'aquesta integració.*

2. La guerra a Ucraïna i la penetració d'empreses israelianes per l'Est d'Europa:

La guerra a Ucraïna funciona com a espai de prova, validació i projecció comercial. Empreses israelianes entren a l'Europa de l'Est mitjançant contractes, aliances industrials, plataformes d'innovació i xarxes de producció. Això reforça la seva posició davant l'OTAN i facilita noves oportunitats comercials en seguretat, drons i tecnologies de doble ús.

3. Alemanya com a epicentre del lobby militar israelià:

Aquest país emergeix com a epicentre del lobby militar israelià a Europa. No només concentra grans contractes i exportacions, sinó també estructures d'influència política, econòmica i mediàtica, com *European Leadership Network* (Xarxa Europea de Lideratge) o *Israel Defence and Security Forum* (Fòrum Israelià de Defensa i Seguretat), que treballen per reforçar la cooperació militar, de ciberseguretat i intel·ligència, i per legitimar Israel com a soci estratègic europeu.

4. Participació a fires de tecnologia i ciberseguretat com a mecanisme per accedir a la UE:

Les fires i congressos tecnològics i de ciberseguretat operen com a mecanismes de legitimació i accés al mercat europeu. Espais com Barcelona, Brussel·les, Madrid, Londres, Nuremberg o Praga permeten a empreses israelianes presentar-se com a actors civils i innovadors, tot difuminant els seus vincles amb la indústria militar i de vigilància.

5. Del soft-landing a Xipre a estructures empresarials opaques:

Xipre apareix com una plataforma de *soft-landing* per a empreses israelianes, gràcies a avantatges fiscals, proximitat geogràfica, flexibilitat reguladora i manca de control efectiu sobre productes de cibervigilància. Aquest entorn facilita la creació d'estructures opaques i la canalització d'operacions comercials dins de la UE.

6. Luxemburg com a plataforma de llançament:

Luxemburg es consolida com a plataforma de llançament d'empreses, amb NSO Group com a cas paradigmàtic. La seva estructura financera i societària hi permet desplegar xarxes hòlding i filials que faciliten facturació, contractació i operacions europees sota una aparença de normalitat empresarial, malgrat els greus antecedents en matèria de programari espia i vulneracions de drets humans.

7. Adquisició d'empreses europees i *rebranding* per operar a la UE:

L'adquisició d'empreses europees i el *rebranding* constitueixen una estratègia clau per operar a la UE. Mitjançant la compra de societats locals, la creació de noves filials o el canvi de marca, empreses israelianes poden accedir a finançament europeu, reduir el cost reputacional i presentar-se com a actors europeus legítims. El cas d'Intracom Defense-IAI n'és paradigmàtic.

8. L'accés a la Unió Europea a través dels programes de finançament:

Els programes europeus de finançament, especialment *Horizon Europe* i l'*European Defence Fund*, funcionen com a porta institucional d'accés. L'estatus d'Israel com a país associat li permet participar en condicions gairebé equivalents a les dels Estats membres, incloent-hi projectes de ciberseguretat, drons i tecnologies de doble ús, tot i els vincles documentats de moltes empreses amb l'aparell militar israelià.

9. Barcelona com a hub tecnològic d'empreses de ciberseguretat:

Barcelona es projecta com a hub emergent de ciberseguretat i, alhora, com a espai d'aterratge d'empreses israelianes o vinculades al seu ecosistema. La combinació d'infraestructura tecnològica, fires internacionals, inversió estrangera i febles mecanismes de supervisió ha convertit la ciutat en una plataforma atractiva per a societats de ciberseguretat, incloses empreses relacionades amb programari espia i explotació de vulnerabilitats.

A partir d'aquesta anàlisi, es proposen les següents recomanacions:

- Introduir clàusules vinculants a la contractació pública europea per excloure empreses implicades en vulneracions greus dels drets humans, amb mecanismes de verificació i control basats en fonts fiables.
- Reforçar el Reglament 2021/821 del Parlament Europeu, que estableix un règim de control de les exportacions, el corretatge, l'assistència tècnica, el trànsit i la transferència de productes de doble ús, per impedir exportacions amb risc de repressió o vigilància, harmonitzant criteris i evitant l'elusió de controls.
- Prohibir el desenvolupament, comercialització i ús de programari espia, així com el comerç d'*exploits* fora d'usos de seguretat.
- Adoptar sancions específiques contra Israel i entitats implicades, incloent-hi restriccions econòmiques i limitacions d'accés al mercat europeu.
- Establir un embargament integral d'armes a Israel, incloent tecnologies de doble ús, amb mesures per prevenir l'elusió, és a dir, per evitar que es pugui esquivar mitjançant intermediaris o vies indirectes.
- Reforçar la supervisió d'inversions vinculades a empreses amb risc de contribuir a vulneracions greus, amb criteris harmonitzats a la UE.
- Exigir diligència reforçada a actors financers, incloent anàlisi de beneficiaris finals, cadenes de valor i estructures opaques.
- Imposar transparència i auditoria en acords tecnològics i militars, i detectar rebranding i estructures opaques.
- Excloure dels programes de finançament de la Unió Europea aquelles empreses implicades en vulneracions greus de drets humans, amb l'ampliació dels criteris d'elegibilitat i el reforç dels mecanismes de seguiment i control dels projectes.