

SICUREZZA ECONOMICA

Imprese e università europee davanti all'intelligence cinese: cosa rischiano davvero

La gran parte della letteratura è americana e riflette una scala che l'Europa non ha. Serve una traduzione, non un trasferimento. Guida ragionata ai rischi — e agli strumenti che oggi non li presidiano.

di Carmine Di Marino

Il problema, ridotto all'osso, è uno solo: a un avversario integrato per costruzione dottrinale — che non separa sicurezza e sviluppo, civile e militare, impresa e Stato — corrisponde in Europa un difensore frammentato per costruzione istituzionale. Cybersicurezza, protezione del patrimonio informativo, valutazione della controparte e conformità sono funzioni distinte, che non condividono dati né vocabolario né catena di riporto. Un avversario integrato che affronti un difensore frammentato attacca, prevedibilmente, le giunture.

Le tre asimmetrie europee

Prima di importare ricette americane conviene misurare tre differenze. L'esposizione economica: la Cina è il principale partner per le importazioni, e il costo di un disaccoppiamento sarebbe incomparabilmente superiore a quello statunitense. L'architettura istituzionale: la sicurezza nazionale resta competenza degli Stati membri ai sensi dell'art. 4, par. 2, TUE, sicché l'Unione agisce per vie indirette. E la posizione: l'Europa non è il bersaglio principale della competizione sino-americana, ma ne è il terreno. Da qui la formula: una traduzione, non un trasferimento.

Sicurezza economica e il limite del «de-risking»

La sicurezza economica è entrata nel lessico dell'Unione con la strategia del giugno 2023 (valutare, proteggere, promuovere). La formula «de-risking, non decoupling» merita però un esame severo: è più una posizione negoziale che una dottrina, perché manca una definizione operativa del rischio da ridurre, della soglia accettabile e soprattutto di chi ne sopporti il costo — che oggi grava sull'impresa.

Gli strumenti presidiano il controllo; la minaccia opera sulla disponibilità

Gli strumenti giuridici disponibili — controllo degli investimenti in entrata (regolamento UE 2019/452 e, in Italia, golden power), controllo delle esportazioni dual-use, controllo degli investimenti in uscita — condividono un limite di fondo: presidiano il controllo societario, mentre il quadro cinese opera sulla disponibilità. Un'impresa cinese che divenga fornitore critico o partner di ricerca, senza acquisire

partecipazioni, resta fuori dal perimetro del controllo e dentro quello dell'art. 7 della National Intelligence Law. La soglia partecipativa è un criterio disallineato rispetto alla minaccia.

Due diligence, M&A e il rischio che nessuno prezza

La revisione della Counter-Espionage Law del 2023 ha reso giuridicamente rischiosa, in Cina, l'attività ordinaria di raccolta su una controparte. Ne discende un'asimmetria da enunciare senza eufemismi: l'acquirente o il partner europeo non può condurre sulla controparte cinese la due diligence che questa può condurre su di lui. Il rischio va prezzato o strutturato — dichiarazioni e garanzie sui rapporti con l'apparato di sicurezza, escrow, clausole risolutive collegate a designazioni in liste di misure restrittive, segregazione del patrimonio informativo. I profili da presidiare non coincidono con quelli tradizionali: titolarità effettiva, presenza del comitato di Partito nella controparte, partecipazioni sotto soglia e, soprattutto, i canali non proprietari — licenze, joint venture con trasferimento di know-how. Il canale più pericoloso non è l'intrusione informatica, ma l'assunzione dell'ingegnere che possiede la conoscenza tacita di processo: un rischio che nessun controllo sugli investimenti presidia, e che si governa solo con strumenti di diritto del lavoro e cultura organizzativa.

Le università, dove l'errore è più probabile

L'università è il soggetto in cui l'errore di impostazione è più probabile, in due direzioni opposte. Il primo errore è la negazione del problema — la tesi che la ricerca sia per definizione aperta — che ignora la natura a duplice uso di parte della ricerca contemporanea e l'esistenza di atenei cinesi collegati alla difesa. Il secondo è l'eccesso opposto: la China Initiative statunitense, chiusa nel febbraio 2022 dopo esiti processuali largamente negativi, mostra che un criterio fondato sulla nazionalità produce falsi positivi, distrugge la cooperazione scientifica e induce alla fuga i ricercatori che si intendeva trattenere. L'impostazione difendibile è basata sul rischio della linea di ricerca e non sulla persona: classificare le linee per sensibilità, presidiare i punti in cui la conoscenza esce, esigere trasparenza degli impegni esterni da chiunque, dotarsi di una funzione di research security di supporto e non di polizia.

Il punto d'ingresso che nessuno presidia

Sul piano tecnico, il quadro europeo — NIS 2, resilienza dei soggetti critici, Cyber Resilience Act, DORA per il settore finanziario — è coerente ma sconta tre limiti che i casi Volt e Salt mettono a fuoco. Primo: entrambe le campagne entrano dallo stesso punto, l'apparato di frontiera, che nella gran parte delle organizzazioni non ospita strumenti di rilevamento, non figura nei programmi di aggiornamento e spesso ha superato il termine di supporto; è statisticamente il punto più rilevante, e nessuno strumento europeo lo presidia specificamente. Secondo: la difesa dal *living off the land* non è alla portata dell'operatore di piccole dimensioni, che nel tessuto produttivo italiano è la regola — l'unica via praticabile è la mutualizzazione (servizi gestiti, consorzi settoriali, capacità condivise). Terzo: sostituire un fornitore di componentistica di rete non risolve il problema strutturale, poiché gli apparati compromessi erano in maggioranza di costruttori occidentali e la vulnerabilità sfruttata era nota.

NATO, la soglia e la funzione di raccordo

La NATO ha riconosciuto il cibernazio come dominio operativo nel 2016 e affermato che un attacco cibernetico può, caso per caso, condurre all'invocazione dell'art. 5. Ma il pre-positioning si colloca, per costruzione, sotto qualunque soglia: non produce effetti e dunque non attiva alcuna clausola. È la ragione per cui la leva realmente disponibile non è la deterrenza per punizione, ma la resilienza. L'implicazione più importante, però, è organizzativa: non imitare il modello cinese — la frammentazione europea è il prezzo e il prodotto della separazione dei poteri, che è l'oggetto stesso della difesa — ma dotarsi delle giunture mancanti. Una funzione di raccordo, che nella tradizione francese si chiama intelligence economica, capace di collegare ciò che l'analista di sicurezza osserva sulla rete con ciò che il negoziatore osserva al tavolo, riportata al vertice e non a una direzione tecnica. Perché nessuna delle campagne esaminate è stata resa possibile da una tecnologia inaccessibile: solo da apparati non aggiornati, credenziali riutilizzate, log non conservati. La cultura della sicurezza è la condizione perché l'inventario degli apparati esposti diventi una questione da consiglio di amministrazione, e non un dettaglio della manutenzione.

Fonti principali

Commissione UE e Alto rappresentante, JOIN(2023) 20 final, «Strategia europea di sicurezza economica», 20 giugno 2023.

Regolamento (UE) 2019/452 (screening IDE); Regolamento (UE) 2021/821 (dual-use); d.l. 21/2012 (golden power).

Direttiva (UE) 2022/2555 (NIS 2) e d.lgs. 138/2024; Regolamento (UE) 2024/2847 (Cyber Resilience Act); DORA.

U.S. Department of Justice, dichiarazione sulla conclusione della China Initiative, 23 febbraio 2022.

A. Joske, The China Defence Universities Tracker, Australian Strategic Policy Institute, 2019.