

APPARATI DI INTELLIGENCE

Chi è davvero il Ministero della Sicurezza di Stato cinese

Nessun bilancio pubblico, nessun controllo parlamentare, una struttura ricostruita per induzione. Ritratto dell'agenzia che fonde spionaggio, sviluppo tecnologico e sicurezza politica — e che non ha equivalenti in Occidente.

di Carmine Di Marino

Il Ministero della Sicurezza di Stato (MSS) è il principale organismo di intelligence civile della Repubblica Popolare Cinese, e insieme uno dei più opachi. Non è soggetto a controllo parlamentare, non pubblica bilanci, e la sua struttura è stata ricostruita in gran parte per via induttiva, incrociando ricostruzioni da fonti aperte, documentazione fuoriuscita e atti giudiziari occidentali. Istituito nel 1983 dalla V Assemblea nazionale del popolo, nasce dalla fusione delle componenti di controspionaggio del Ministero della Pubblica Sicurezza con il Dipartimento centrale di investigazione del PCC.

Un'agenzia senza equivalenti

La sua specificità sta nella concentrazione di funzioni che, nelle democrazie liberali, sono normalmente distribuite: intelligence esterna, controspionaggio e sicurezza interna. In Italia il sistema è duale — AISE e AISI, coordinate dal DIS; negli Stati Uniti le funzioni sono ripartite tra CIA, FBI e altre componenti. Il MSS, sotto questo profilo, non ha equivalenti nelle democrazie occidentali: riflette un modello in cui la distinzione tra Stato, Partito e apparato di sicurezza è assai meno netta.

Un potere decentrato

Un tratto strutturale, spesso trascurato, è il decentramento. Il MSS dispone di dipartimenti provinciali e uffici municipali dotati di rilevante autonomia; la maggior parte delle campagne informatiche attribuite al Ministero è riconducibile a uffici periferici — Tianjin, Jiangsu, Sichuan, Guangdong, Hainan — ciascuno con la propria rete di appaltatori. L'unico ufficio di cui è documentata pubblicamente l'esistenza è l'undicesimo, operante come CICIR, l'istituto di ricerca collegato al Ministero.

Il modello a contractor

L'elemento di maggiore specificità dell'operatività cyber del MSS è il ricorso sistematico ad appaltatori privati. La campagna APT10 (Cloud Hopper) è stata legata, da un atto d'accusa statunitense del 2018, all'MSS e a una sua società-schermo, la Huaying Haitai di Tianjin. Una conferma più ampia è arrivata nel febbraio 2024, quando una mole di documenti interni della società i-Soon (Anxun) è comparsa su una piattaforma pubblica di condivisione del codice: listini, cataloghi di strumenti offensivi e corrispondenza che documentano la vendita di capacità di intrusione a committenti

pubblici cinesi. Il modello consente scala, costi ridotti e negabilità; ma proprio l'esternalizzazione genera vulnerabilità — leak, tracciabilità dei fornitori, esposizione ad atti giudiziari. L'ecosistema cyber cinese non è monolitico: è reticolare, scalabile e, per ciò stesso, più esposto a errori e attribuzioni.

L'uomo resta al centro

Nonostante la crescita del dominio cyber, il nucleo del MSS resta la raccolta HUMINT, condotta con orizzonti di lungo periodo. Il caso più eloquente è quello di Xu Yanjun, ufficiale del Dipartimento della sicurezza di Stato del Jiangsu, arrestato in Belgio nel 2018, estradato negli Stati Uniti e condannato per spionaggio economico ai danni di GE Aviation e Safran: la prova diretta del legame, centrale in tutta l'analisi, tra intelligence e sviluppo tecnologico. Vi si affiancano le vicende di Kevin Mallory e Jerry Chun Shing Lee, ex ufficiali della CIA, e sul fronte opposto lo smantellamento di una rete informativa statunitense in Cina tra il 2010 e il 2012.

Il canale accademico

Un'ulteriore forma di reclutamento passa per l'università: i programmi di attrazione dei talenti, gli atenei legati alla difesa — i cosiddetti «sette figli della difesa nazionale» — e la collaborazione ordinaria di dottorandi e visiting professor. Il MSS dispone così di un accesso al tessuto tecnologico nazionale che non ha equivalenti nei servizi occidentali; lo strumento attraverso cui questa capacità si è espressa nell'ultimo decennio è il cyber espionage.

NOTA DI METODO

Sul MSS ogni affermazione va calibrata sulla fonte. L'esistenza dell'undicesimo ufficio è un fatto documentato; il collegamento di APT10 all'ufficio di Tianjin è un'attribuzione giudiziaria; l'ampiezza e l'architettura della rete di contractor sono una valutazione analitica costruita per induzione. Tenere insieme i tre livelli senza confonderli è la sola difesa contro la sovra-interpretazione di un oggetto per sua natura opaco.

Fonti principali

P. Mattis, M. Brazil, Chinese Communist Espionage: An Intelligence Primer, Naval Institute Press, 2019.
United States v. Zhu Hua and Zhang Shilong, S.D.N.Y., 17 dicembre 2018 (APT10 / Cloud Hopper).
United States v. Xu Yanjun, S.D. Ohio, 2018-2022 (spionaggio economico GE Aviation / Safran).
SentinelOne e NattoThoughts, analisi sui documenti i-Soon / Anxun, febbraio-marzo 2024.
M. Mazzetti et al., «Killing C.I.A. Informants...», The New York Times, 20 maggio 2017.