START/INSIGHT
STRATEGIC ANALYSTS AND RESEARCH TEAM
www.startinsight.eu – info@startinsight.eu

La nuova strategia di intelligence USA: implicazioni per il Sistema di Informazioni e Sicurezza della Repubblica.

di *Niccolò Petrelli*, Ricercatore associato START InSight, Ricercatore Università Roma 3

Per citare questo articolo: Niccolò Petrelli (2024): *La nuova strategia di intelligence USA: implica-zioni per il Sistema di Informazioni e Sicurezza della Repubblica*, START InSight.

https://www.startinsight.eu/**la-nuova-strategia-di-intelligence-usa/**

Abstract (Italian)
Nell'agosto 2023 l'US Office of the Director of National Intelligence (ODNI) ha pubblicato una National Intelligence Strategy (NIS) incentrata sulla nuova era di competizione con la Cina che nel corso degli ultimi mesi ha iniziato ad essere attuata. Esiste la possibilità che la strategia di collega-mento USA si traduca in opportunità per il sistema d'intelligence italiano? La disanima di Niccolò Petrelli è strutturata in modo tale da dare una risposta all'importante quesito.

Keywords: AISE, AISI, *intelligence*, CIA, DIS, NIS, ODNI, SISR.

Nell'Agosto 2023 l'*US Office of the Director of National Intelligence* (ODNI) ha pubblicato una *National Intelligence Strategy* (NIS) incentrata sulla nuova era di competizione con la Cina che nel corso degli ultimi mesi ha iniziato ad essere attuata.[1] Uno degli elementi centrali del documento, che essenzialmente delinea la visione per il futuro dell'ODNI più che una vera e propria strategia, è la decisione di rafforzare ed espandere la rete internazionale di "collegamenti" con altri servizi informativi (nonché con vari tipi di attori privati).[2] Quale l'eventuale impatto sul Sistema di Informazioni e Sicurezza della Repubblica (SISR)? Esiste la possibilità che la strategia di collegamento USA si traduca in opportunità per il sistema d'*intelligence* italiano?

Per rispondere a queste domande è possibile partire da un precedente analogo nella storia dell'*intelligence* USA. Tra la seconda metà del 1945 e la prima metà del 1947 infatti, l'emergere della competizione con l'Unione Sovietica spinse l'apparato informativo statunitense ad investire in maniera sistematica risorse, capacità, *expertise*, e relazioni personali nella creazione di una massiccia e stratificata infrastruttura di collegamenti con i servizi segreti di numerosi paesi dell'Europa occidentale.[3] In un

[1] https://oversight.house.gov/wp-content/uploads/2024/05/05062024-ODNI-Letter.pdf.

[2] https://www.voanews.com/a/new-us-intelligence-strategy-calls-for-more-partners-more-sharing-/7220725.html

[3] Michael Warner AID

primo momento a guidare tale strategia furono principalmente requisiti di "accesso" e ampliamento della raccolta informativa sull'URSS e i suoi "alleati" in Europa orientale: i paesi dell'Europa occidentale rappresentavano infatti quella che potremmo definire la più valida "piattaforma" per accedere a tali obiettivi informativi. Nel 1946 ad esempio fu raggiunto un tacito accordo in base al quale la MUST e la FRA, le due agenzie di *intelligence* militare svedesi, iniziarono a passare all'*intelligence* USA tutti le informazioni di HUMINT e SIGINT sulle attività militari sovietiche nella regione baltica in cambio di finanziamenti e equipaggiamento per la raccolta informativa tecnica. Un altro esempio, più noto, è quello dell'accordo UKUSA, sempre del 1946, in base a cui la *State-Army-Navy Communications Intelligence Board* degli Stati Uniti e la *London SIGINT Board* si impegnavano a condividere ogni prodotto informativo di raccolta tecnica, mettendo di fatto in piedi una ripartizione del lavoro che l'ex direttore del *Government Communications Headquarters* (GCHQ) David Omand ha definito basata sui "soldi statunitensi e cervelli britannici".[4]

La situazione iniziò tuttavia a cambiare approssimativamente dal 1949. L'*intelligence* americana modificò progressivamente la propria azione di collegamento, strutturandola in base alla percezione della natura della competizione prevalente a Washington, ovvero quella di un confronto in primo luogo politico-ideologico con l'URSS. Ciò si riteneva richiedesse una fusione dei paradigmi strategici di "guerra" e "pace" in uno sforzo unitario e coordinato di *political warfare,*[5] come la definì George Kennan. Tanto la CIA quanto le varie componenti dell'*intelligence* militare intensificarono dunque le proprie attività di collegamento in Europa occidentale promuovendo, in modi e forme diverse a seconda delle circostanze, lo sviluppo di tutte quelle capacità ritenute essenziali per gestire il nuovo tipo di confronto: propaganda, guerra psicologica, sostegno clandestino a forze politiche locali e, qualora necessario, contro-guerriglia.[6] In Germania ad esempio, oltre alla creazione di diverse reti *stay-behind* (S/B), documentazione recentemente declassificata ha gettato luce sul sostegno fornito dalla CIA e dall'*intelligence* militare USA per attività clandestine condotte dall'Organizzazione Gehlen (la prima struttura di *intelligence* di quella che sarebbe diventata la Repubblica Federale Tedesca), al fine di minare la stabilità della zona di occupazione sovietica della Germania.[7] Dove si rivelò più difficile cooperare ad ampio spettro con le controparti locali la comunità di *intelligence* statunitense combinò attività di collegamento ad operazioni clandestine. Un approccio di questo tipo fu adottato ad esempio in Italia, dove dalla fine della Seconda Guerra Mondiale l'*intelligence* americana operò simultaneamente a due diversi livelli: da un lato collaborando con i servizi segreti italiani, in particolare nel programma S/B, dall'altro sviluppando autonomamente reti clandestine per condurre attività di guerra psicologica, propaganda e destabilizzazione.

La strategia di collegamento USA generò dunque effetti trasformativi della struttura, capacità, e funzioni degli apparati informativi europei occidentali, rischi di vario tipo, basti pensare proprio al caso dell'Italia, ma anche oppor-

[4] https://media.defense.gov/2021/Jul/15/2002763709/-1/-1/0/AGREEMENT_OUTLINE_5MAR46.PDF; https://www.securityweek.com/britains-gchq-listening-post-tune-nsa.

[5] George F. Kennan, *The Inauguration of Organized Political Warfare* [Redacted Version], 30 aprile 1948, Woodrow Wilson Center, History and Public Policy Program Digital Archive, https://digitalarchive.wilsoncenter.org/document/114320.pdf?v=94.

[6] US Department of State, *Foreign Relations of the United States*, *1951*, *Vol. I, National Security Affairs, Foreign Economic Policy*, Washington DC, Government Printing Office, 1979 (FRUS 1951), Doc. 18 *Attachment to Memorandum for the National Security Council by the Executive Secretary*, 8 maggio 1951.

[7] https://nsarchive.gwu.edu/briefing-book/openness-russia-and-eastern-europe-intelligence/2022-05-11/secret-war-germany-cias.

tunità, in particolare di beneficiare di finanziamenti, anche cospicui, nonché di forniture di equipaggiamento tecnologicamente avanzato. Non tutti i servizi europei occidentali tuttavia furono parimenti in grado di sfruttare tali opportunità. Ciò dipese da variabili di vario tipo legate al contesto, la natura delle relazioni diplomatiche con gli USA, il grado di fiducia esistente tra i decisori politici ed i vertici degli apparati informativi, la condizione politica prodotta dalla Seconda Guerra Mondiale e, non da ultimo, la posizione geografica dei vari paesi rispetto agli obiettivi informativi di prioritario interesse per la comunità d'*intelligence* USA. Di cruciale importanza furono tuttavia anche taluni fattori squisitamente materiali, ovvero il grado di "interoperabilità" con il sistema d'*intelligence* statunitense, l'adattabilità e funzionalità delle capacità, esistenti e potenziali, dei servizi dell'Europa occidentale rispetto alle missioni affidate al sistema d'*intelligence* USA nel quadro della *political warfare* nei confronti del blocco comunista, e da ultimo la complementarietà di capacità e competenze rispetto a quelle espresse dalle varie componenti del sistema USA.

Il GCHQ britannico fu ad esempio in grado, capitalizzando sulle proprie competenze specifiche in termini di analisi politica del sistema internazionale e crittoanalisi, nonché sulla "interoperabilità" tecnica con il sistema USA, di massimizzare i vantaggi derivanti dalla strategia di collegamento attuata dagli USA arrivando, come visto sopra, a siglare un accordo che garantiva accesso ad ogni prodotto (in teoria) di raccolta tecnica statunitense. L'*intelligence* svedese, da parte sua, riuscì, in particolare in virtù delle proprie autonome capacità di raccolta tecnica in un'area di cruciale importanza strategica per gli USA, ad assicurarsi finanziamenti e equipaggiamento per rafforzare un settore di raccolta prioritario per la sicurezza nazionale del paese. Il caso italiano dimostra invece come, nonostante l'abilità dimostrata in diverse circostanze dai vertici dell'apparato informativo nello sfruttare a proprio vantaggio la propensione USA ad intensificare i collegamenti, come ad esempio nel caso del programma congiunto S/B Italia-USA "Gladio" avviato nel 1951, limiti capacitivi impedirono di cogliere ulteriori potenziali opportunità. Infatti, le scarse competenze analitiche dell'*intelligence* italiana, in particolare sotto il profilo economico, sociologico e politologico, e la conseguente incapacità di sviluppare analisi ad ampio spettro della base di sostegno e infrastruttura sociale del Partito Comunista Italiano (PCI) contribuì in maniera non trascurabile a far sì che l'*intelligence* USA procedesse in maniera autonoma sia alla raccolta informativa che ad una serie di attività operative di contrasto nei confronti del PCI.[8] Allo stesso modo la mancanza di una solida capacità di raccolta SIGINT da parte dell'apparato informativo italiano precluse l'opportunità, intorno alla metà degli anni '50, nel momento in cui Washington era particolarmente interessata a monitorare l'intensificazione dell'attività navale sovietica nel Mediterraneo, di estendere i collegamenti con il sistema d'*intelligence* USA a condizioni vantaggiose per l'Italia, e rappresentò molto probabilmente una delle ragioni alla base della creazione da parte statunitense nel 1960 di una struttura SIGINT gestita dall'*Air Force Security Group* (USAFSS) a San Vito dei Normanni.[9]

Basandoci su quanto sopra, si può ipotizzare che l'attuazione della strategia di collegamento delineata nella NIS 2023 presenterà per l'apparato informativo italiano, con buona probabilità, opportunità analoghe a quelle che emersero al principio della Guerra Fredda. Due sono dunque gli elementi su cui concentrare l'attenzione per comprendere come esse potrebbero essere sfruttate nella maniera più efficace: il primo è la percezione USA della natura della

[8] Niccolò Petrelli, "Alcide De Gasperi e le Origini del Servizio Informazioni Forze Armate (SIFAR)", in Mario Caligiuri (a cura di) De Gasperi e L'Intelligence (in corso di pubblicazione).

[9] https://www.cia.gov/readingroom/docs/DOC_0000278476.pdf

competizione con la Cina, il secondo sono le capacità (a livello aggregato) che i vertici dell'*intelligence* USA stanno sviluppando ed intendono promuovere per i prossimi anni.

Per quanto riguarda il primo elemento, dopo un periodo piuttosto lungo di dibattito, la natura della competizione con la Cina ha iniziato ad essere definita con maggiore precisione. Benché l'assunto di partenza rimanga quello di una competizione globale in ogni ambito, economico, politico, sociale, dell'informazione, e militare, è recentemente emerso un consenso sempre più ampio circa il fatto che la componente centrale di tale competizione sia di natura tecnologico-economica.[10] In altre parole, si ritiene che essa sia incentrata sulla creazione di un vantaggio competitivo duraturo nelle principali tecnologie di frontiera, intelligenza artificiale generale, microprocessori e reti di comunicazione di prossima generazione, produzione avanzata, stoccaggio e produzione di energie, biotecnologie, al fine di poter plasmare l'economia globale della prossima generazione e definire gli standard di accesso e impiego a tali tecnologie.[11]

In merito al secondo elemento, per comprendere il tipo di capacità che l'ODNI intende promuovere nella comunità d'*intelligence* USA è possibile fare riferimento alla nozione di *Revolution in Intelligence Affairs* (RIA), da alcuni anni ormai popolare nel dibattito professionale e politico USA sull'*intelligence*. Benché nella NIS non vi siano espliciti riferimenti al concetto, appare evidente come la RIA rappresenti il costrutto-guida *de facto* impiegato per coordinare una serie di trasformazioni, nel *procurement* e integrazione di nuove tecnologie, nella struttura organizzativa, e nelle procedure operative del sistema d'*intelligence* USA, al fine di porlo nelle condizioni migliori per affrontare le sfide dei prossimi decenni, in primis quelle legate alla competizione con la Cina.

La trasformazione immaginata dall'ODNI prevede di procedere in primo luogo all'acquisizione e integrazione su vasta scala di intelligenza artificiale, sensori all'avanguardia e tecnologie di automazione, evitando approcci incrementali o settoriali. Simultaneamente, alla luce della velocità, della scala, e della complessità a cui opereranno queste tecnologie, verranno promossi rapidi cambiamenti organizzativi e operativi volti ad agevolare forme di integrazione tra raccolta e analisi, promuovere ridondanza tra le varie fasi del ciclo di *intelligence*, nonché a creare meccanismi più rapidi per la diffusione in tempo reale dei prodotti informativi. In altre parole, si intende promuovere un modus operandi "a rete" per il sistema di *intelligence* basato sulla fusione completa dei flussi di dati prodotti da ogni tipo di sensori e piattaforme, la sincronia e integrazione di tutte le attività operative, e la trasmissione rapida e continua di prodotti a operatori umani, macchine e decisori in tutti i dominii.[12]

Quali dunque le capacità e competenze su cui il SISR dovrebbe puntare per essere in grado di cogliere le opportunità generate dalla strategia di collegamento dell'*intelligence* USA? Essenziale è che esse rispondano alla percezione della competizione come di un confronto essenzialmente tecno-economico, e che siano complementari alle capacità espresse dal sistema d'intelligence USA.

In primo luogo dunque il SISR dovrebbe rafforzare le proprie capacità di raccolta e analisi in ambito economico e tecnologico. La questione non è nuova, il dibattito sul rafforzamento dell'*intelligence* economica risale agli

[10] *Intelligence Innovation. Repositioning for Future Technology Competition*, Second Intelligence Interim Panel Report (IPR) of the Special Competitive Studies Project (SCSP), Aprile 2024.
[11] Brandon Kirk Williams, *The Innovation Race: US-China Science and Technology Competition and the Quantum Revolution* (Washington DC: Woodrow Wilson Center, 2023).
[12] *Creating Cross-Domain Kill Webs in Real Time*, DARPA (Sept. 18, 2020), https://www.darpa.mil/news-events/2020-09-18a e *AI Fusion: Enabling Distributed Artificial Intelligence to Enhance Multi-Domain Operations & Real-Time Situational Awareness*, Carnegie Mellon University (2020), http://www.cs.cmu.edu/~ai-fusion/overview.

anni 90, con il lavoro delle commissioni Ortona (1992) e Jucci (1997).[13] Approssimativamente nello stesso periodo inoltre in seno al Comitato Esecutivo per i Servizi di Informazione e Sicurezza (CESIS) fu attivato un "gruppo permanente per l'intelligence economica". Di recente l'ex direttore del SISDE Mori ha rilanciato l'idea di un organismo collegiale dove siano rappresentati il Dipartimento delle Informazioni per la Sicurezza (DIS), le due agenzie (Aisi e Aise), i ministeri interessati e le associazioni degli imprenditori. Nel caso specifico tuttavia la questione chiave sarebbe, in coerenza con quello che è l'approccio USA all'*intelligence* economico-tecnologica, adottare una postura proattiva, che includa attività offensive su base continuativa nei confronti non solo della Cina e dei suoi principali partner economici e tecnologici, ma anche di imprese e enti privati riconducibili a quello che potremmo chiamare "l'ecosistema tecno-economico" cinese.

In secondo luogo, il SISR dovrebbe investire sullo sviluppo ulteriore delle proprie capacità operative in aree in cui gode di un vantaggio competitivo, ed in cui esse possano impiegarsi in maniera complementare a quelle del sistema d'*intelligence* statunitense. La scelta più logica appare l'area del Mediterraneo, dove da diversi decenni ormai il sistema d'*intelligence* italiano conduce attività operativa di ampio respiro. Proprio nel Mediterraneo infatti negli ultimi anni la Cina ha, con discrezione, ampliato la propria presenza attraverso grandi aziende private (Shanghai International Port Group, China Merchants) e pubbliche (COSCO, China Communications and Construction Company) stipulando accordi commerciali di vario tipo, accordi per partecipazioni nei porti di paesi situati lungo rotte marittime vitali per la Belt and Road Initiative, e acquisendo aziende di medie dimensioni, spesso allo scopo di avere accesso a tecnologie Europee.[14]

Il necessario presupposto ovviamente, come evidenziano gli esempi di UK e Svezia durante la Guerra Fredda, è che il sistema d'*intelligence* italiano goda di un buon livello di "interoperabilità" con quello USA. Ciò, a sua volta, richiede che i vertici dell'apparato informativo proseguano, e auspicabilmente diano ulteriore impulso, a quel processo di acquisizione e integrazione di tecnologie dell'informazione di ultima generazione, sensori avanzati, Intelligenza Artificiale e sistemi di apprendimento automatico, che sembra essere iniziato da qualche anno.

Niccolò Petrelli è Ricercatore presso il Dipartimento di Scienze Politiche dell'Università Roma Tre, dove insegna Studi Strategici, e Senior Researcher per StartInsight.

info@startinsight.eu

[13] Gabriele Carrer, Perché all'Italia serve intelligence economica. Intervista al generale Mori, Formiche 9 Giugno 2024 https://formiche.net/2024/06/intervista-intelligence-economica-mario-mori/#content..

[14] Claudia De Martino, The Growing Chinese Presence in the Mediterranean, Med-Or Geopolitics, 22 April 2024, https://www.med-or.org/en/news/la-crescente-penetrazione-cinese-nel-mediterraneo.