L'*intelligence* e le sfide poste dalle nuove tecnologie

Intelligence e sovrabbondanza di informazioni

Nella nostra epoca i servizi di *intelligence* devono operare in un ambiente in cui informazioni e comunicazioni abbondano, specialmente online. A titolo di esempio, si stima che ogni giorno gli utenti di internet si scambino centinaia di milioni di e-mail. La mole di informazioni sul web tende, peraltro, a crescere sensibilmente ogni anno. Tutto ciò fa sì che le agenzie di *intelligence*, anche degli Stati più potenti come gli USA, già oggi raccolgano più informazioni di quanto gli attori umani possano effettivamente elaborare e analizzare (Zegart 2023, 64).

Questa tendenza rischia di accentuare il ben noto problema del «rapporto tra "segnale" e "rumore"» (*signal to noise ratio*) (in particolare, Wohlstetter 1962): le poche informazioni vere e rilevanti (*signal*) sono sempre più sommerse da una massa di informazioni irrilevanti e/o false (*noise*) (si veda anche Marone 2011, 264).

Intelligence e nuove tecnologie

Le nuove tecnologie hanno evidentemente giocato un ruolo centrale in questa evoluzione. Lo sviluppo di internet e, in particolare, dei *social media* ha effetti assai rilevanti sulle attività di raccolta e analisi delle informazioni svolte dai servizi di *intelligence*. A queste tecnologie si aggiungano quelle che stanno emergendo o stanno consolidandosi in questi anni, come l'intelligenza artificiale (tra i molti altri, Kissinger et al. 2021) e la computazione quantistica. Queste tecnologie potrebbero essere impiegate anche da Stati ostili, ma anche da attori non-statali con intenzioni malevoli come organizzazioni terroristiche (per esempio, Cronin 2019).

Intelligence e partnership con attori esterni

A differenza di quanto avvenuto nei decenni precedenti, molte di queste tecnologie sono sviluppate nel settore privato. Questo fatto può suggerire il rafforzamento della cooperazione tra apparati statali di *intelligence* e rilevanti attori non-governativi, comprese imprese private. A titolo di esempio, la recente *2023 National Intelligence Strategy* della Comunità di *Intelligence* degli Stati Uniti, pubblicata il 9 agosto 2023, sottolinea l'esigenza di «diversificare, espandere e rafforzare partnership» con attori esterni, «specialmente con attori non-statali e sub-statali» (DNI 2023, 11).

Il ruolo di attori privati nella raccolta e analisi di informazioni

Le nuove tecnologie non di rado sono associate a soglie di accesso non elevate: in altri termini, possono essere acquisite e utilizzate da un numero ampio di organizzazioni, gruppi e persino singoli individui, senza la necessità di grandi investimenti economici e senza il requisito di sofisticate competenze specialistiche.

Nel campo della raccolta e analisi delle informazioni, questa condizione fa sì che anche attori diversi dalle agenzie di *intelligence* statali possano svolgere attività con salienti conseguenze politiche. Si pensi, in particolare, al ruolo di organizzazioni private, gruppi di cittadini o singoli individui che si impegnano a raccogliere e analizzare informazioni in merito a fatti rilevanti della politica internazionale come conflitti armati o incidenti internazionali (Zegart 2023).

Il caso di Bellingcat

A questo riguardo, un caso di particolare interesse è quello offerto da Bellingcat, l'influente organizzazione non-governativa di «indagini online», specializzata in attività di cosiddetta *open-source intelligence* (OSINT) e di *fact-checking*. Costituita da volontari attivi in vari Paesi, Bellingcat

è stata significativamente definita dal suo fondatore - l'ex *blogger* e *citizen journalist* britannico Eliot Higgins -, un'«agenzia di *intelligence* per le persone» (*an intelligence agency for the people*) (Higgins 2021). Alcune delle più note indagini dell'organizzazione hanno riguardato la guerra civile siriana, la guerra in Ucraina, l'avvelenamento di Aleksej A. Naval'nyj e di altri cittadini russi (Higgins 2021).

La frontiera dell'*intelligence* da forti aperte

L'ampia disponibilità di informazioni nella nostra epoca può suggerire anche un ricorso crescente alla cosiddetta *intelligence* da fonti aperte (OSINT) (cfr. Miller 2018). Negli ultimi anni diversi studiosi ed esperti hanno sottolineato questo aspetto. Amy Zegart, autorevole studiosa statunitense di *intelligence*, si è spinta sino a suggerire l'istituzione di un'apposita agenzia di intelligence specializzata in OSINT per il suo Paese (Zegart e Morell 2019; Zegart 2023). Pur consapevole della complessa articolazione della Comunità di *intelligence* degli Stati Uniti – oggi già costituita da ben diciotto agenzie diverse («*elements*») –, Zegart ha sostenuto che una nuova apposita agenzia, meno vincolata alla tradizionale «cultura della segretezza» dell'*intelligence* (cfr. Mutti 2015), sarebbe nelle condizioni di sviluppare una cooperazione più stretta e sistematica con attori esterni, come imprese private e università, e di sperimentare tecnologie e metodi innovativi, utili per l'intera Comunità di *Intelligence* nazionale.

Conclusioni

Le nuove tecnologie, comprese quelle dell'informazione e della comunicazione, pongono nuove sfide e opportunità ai servizi di *intelligence*. Secondo alcuni studiosi ed esperti, l'adattamento a questo ambiente da parte delle agenzie di *intelligence* potrebbe fondarsi anche su un rapporto più stretto e continuativo con attori esterni, come imprese private, università e *think tanks*.

Bibliografia

- Cronin A. K. (2019). *Power to the people: How open technological innovation is arming tomorrow's terrorists*. Oxford: Oxford University Press.
- DNI (2023). 2023 National Intelligence Strategy. Director of National Intelligence (DNI). testo disponibile al sito: https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2023/item/2402-2023-national-intelligence-strategy (consultato il 5 agosto 2023).
- Higgins E. (2021). *We are Bellingcat: An Intelligence Agency for the People*. London: Bloomsbury Publishing.
- Johnson L. (2017). *National Security Intelligence: Secret Operations in Defense of the*
- *Democracies*. Second Edition. Cambridge: Polity Press.
- Kissinger H., Schmidt E., Huttenlocher D. (2021). *The Age of AI: And Our Human Future*. London: John Murray.
- Marone F. (2017). Perché l'*intelligence* fallisce: il caso dell'11 settembre. *Quaderni di Scienza Politica*, 2: 259-288.
- Miller B.H. (2018). Open source intelligence (OSINT): an oxymoron?. *International Journal of Intelligence and CounterIntelligence*, 4: 702-719.
- Mutti A. (2015). L'organizzazione del segreto nelle agenzie di *intelligence*. *Rassegna Italiana di Sociologia*, 2: 231-258.
- Wohlstetter R. (1962). *Pearl Harbor: Warning and Decision*, Stanford: Stanford University
- Press.
- Zegart A. (2023). Open secrets: Ukraine and the next intelligence revolution. *Foreign Affairs*, 1: 54-70.
- Zegart A. e Morell M. (2019). Spies, lies, and algorithms. *Foreign Affairs*, 3: 85-97.