LUISS

Perché all'Italia servirebbe un Consiglio di Sicurezza Nazionale

di Beniamino Irdi

Policy Brief n. 15/2023

Quattro Paesi del G7 (Stati Uniti, Regno Unito, Francia e Giappone) si sono già dotati di un Consiglio per la Sicurezza Nazionale (CSN), il Canada ne ha recentemente annunciato la costituzione mentre in Germania la discussione politica si è arenata per alcune diatribe fra le forze politiche. Anche in Italia, si argomenta in questo Policy Brief, è necessario un ripensamento dell'architettura di sicurezza nazionale che, conferendo maggior peso ai domini non tradizionali, abbracci l'intera superficie di attacco del Paese. Ad esso deve accompagnarsi un'attività di costante mappatura del reale perimetro della minaccia che rifletta le posizioni dei relativi stakeholder nella formulazione della risposta complessiva del Governo. È dunque inevitabile una riflessione sulla necessità di un punto di fusione costante e permanente delle diverse priorità in una direttrice di governo armonica.

** Una versione ampliata di questo Policy Brief è stata presentata dall'autore lo scorso 20 novembre al workshop "Consiglio per la Sicurezza Nazionale: dovrebbe l'Italia istituirlo?" che si è tenuto al Campus LUISS*

"*Russia is the storm, China is climate change*". "La Russia è una tempesta, la Cina è il cambiamento climatico". Questo è il mantra, un po' semplificatorio, che cattura la natura e la gerarchia delle principali sfide all'Occidente nella percezione degli addetti ai lavori statunitensi e sempre di più anche europei. La tempesta russa scatenatasi il 24 febbraio 2022 con l'invasione dell'Ucraina è una minaccia acuta, violenta, circoscritta nello spazio e nel tempo, oltre che in buona misura convenzionale. La pressione esercitata da Pechino è una sfida sottile, pervasiva e graduale come il cambiamento climatico.
Fino al ritorno della guerra in Europa, lo sguardo dell'Occidente era rivolto verso sfide di lungo periodo. L'approccio transattivo dell'Amministrazione Trump rimetteva in discussione il ruolo della NATO e riportava alla ribalta l'autonomia strategica europea. L'avvento delle reti 5G e la pervasività dell'hardware cinese alimentavano la discussione sulle infrastrutture strategiche che, complice l'ambizione della *Belt and Road Initiative*, avrebbe trovato sempre maggior respiro anche in Europa. La Pandemia da Covid-19 e le sue ricadute economiche e sociali spostavano bruscamente i riflettori dalla dimensione militare della sicurezza nazionale verso quelle non tradizionali come la sanità, l'informazione, il cyber-spazio e l'ingerenza esterna. Complici questi grandi sviluppi, l'establishment della sicurezza statunitense ed europeo metteva gradualmente a fuoco una sfida non nuova, ma resa cogente dal cambiamento dello sfondo strategico, e soprattutto della tecnologia.

Come è cambiato il paradigma delle minacce alla sicurezza

Si tratta della sfida proveniente da attori statuali che, forti di meccanismi decisionali verticistici e dall'assenza di accountability interna, possono avvalersi di tutte le propaggini della società (apparati di sicurezza, aziende, media, diaspore all'estero ecc.) per perseguire obiettivi di proiezione, penetrazione e influenza. Questo sforzo si articola su campagne, talvolta dette "ibride", composte di azioni su diversi domini dello spettro "DIMEFIL" (*Diplomacy, Information, Military, Economic, Financial, Intelligence, Law Enforcement*) e difficili da ricondurre al loro originatore. Le singole azioni sono infatti solitamente negabili, coordinate e sotto la soglia del conflitto armato, e fanno leva sulle fragilità tipiche delle società aperte e sui pesi e contrappesi dei sistemi democratici.

La natura sistemica della minaccia appare più immediatamente evidente da due dei suoi tratti distintivi:
1) **Asimmetria**. Sia le azioni nei singoli domini DIMEFIL che la loro concertazione in campagne sono rese possibili, o almeno molto più economiche, dalle caratteristiche dei sistemi politici da cui promanano e di quelli contro cui sono dirette. Ad esempio, una campagna di disinformazione russa verso l'opinione pubblica europea può contare, per ragioni evidenti, su un alto tasso di segretezza, un pieno allineamento dell'ecosistema mediatico del Paese e un rischio di contraccolpo politico interno sostanzialmente nullo. A fronte di ciò, la sua target audience - l'opinione pubblica europea - è capillarmente esposta a tutti i mezzi di comunicazione e non schermata da forme di controllo o censura governative. Per le ragioni opposte è immediatamente evidente come un'ipotetica campagna di disinformazione occidentale diretta verso l'opinione pubblica russa sia di difficile concepimento, o almeno abbia un rapporto rischi-benefici non particolarmente incoraggiante.

In altre parole, le campagne ibride, o di "*malign influence*" secondo la nomenclatura statunitense, sono costruite appositamente per sfruttare l'estesa superficie di attacco delle democrazie occidentali e le immunità dei loro avversari.
2) **Gradualità/dispersione**. I tasselli delle campagne ibride sono in genere articolati in modo da celare la campagna in cui sono incardinate. Le singole azioni di influenza, oltre a essere spesso messe in atto attraverso proxy per preservare la *deniability* del mittente, possono essere differite nel tempo, nello spazio e nel dominio. Esse hanno sovente come target soggetti non solo diversi ma distanti e non comunicanti, spesso fuori dal radar delle Autorità e degli stessi apparati di sicurezza. Ad esempio, un accordo accademico internazionale di ricerca su un materiale sensibile, un tentativo di acquisizione di un'azienda che lo produce aggirando le restrizioni del golden power e un attacco cyber a un'altra azienda simile per cercare di esfiltrarne il know-how difficilmente saranno messe a sistema dalle Autorità governative per quello che potrebbero essere: un tentativo orchestrato di appropriarsi dell'expertise di un dato Paese in un certo settore. In definitiva, l'originatore della minaccia punta sul fatto che la quantità e varietà di stakeholder del Paese target e la loro indipendenza dalle Autorità governative renda improbabile il raggiungimento di una "massa critica" di informazioni sufficiente a prendere atto della campagna e fare scattare delle contromisure o delle rappresaglie.

Come ripensare l'architettura di Sicurezza nazionale

Dal quadro descritto finora emerge la necessità di un ripensamento del concetto di sicurezza nazionale che, conferendo maggior peso ai domini non tradizionali, abbracci l'intera superficie di attacco del Paese. Ad esso deve accompagnarsi un'attività di continua mappatura del reale perimetro della minaccia che rifletta le posizioni dei relativi stakeholder nella formulazione della risposta complessiva del governo. È dunque inevitabile una riflessione sull'adeguatezza dell'architettura di sicurezza nazionale, e in particolare sulla necessità di un punto di fusione costante e permanente delle diverse priorità in una direttrice di governo armonica.

Rispetto a questa riflessione l'Italia è in ritardo sui suoi principali alleati. Pressoché a fattor comune, essi hanno individuato il punto di fusione in un **Consiglio per la Sicurezza Nazionale (CSN)**. Quattro degli altri sei Paesi del G7 (Stati Uniti, Regno Unito, Francia e Giappone) se ne sono già dotati, il Canada ne ha recentemente annunciato la costituzione mentre in Germania la discussione politica si è arenata sulle dinamiche tattiche fra le forze politiche. In Italia, come altrove, il dibattito sul CSN è stato frenato da dinamiche politiche e obiezioni istituzionali, soprattutto rispetto alla presunta ridondanza di un simile organo con quelli già esistenti e sul rischio di sovrapposizione di competenze con le altre Amministrazioni dello Stato. È effettivamente innegabile che l'architettura istituzionale del Paese sia affollata di comitati, consigli, nuclei, commissioni e organi di coordinamento, ognuno dei quali titolare di una parte dei compiti o delle competenze che spetterebbero a un CSN. L'istituzione di quest'ultimo dovrebbe quindi essere preceduta da un'approfondita riflessione istituzionale, oltre che da una razionalizzazione di ciò che già esiste, al fine di ottimizzare le risorse e massimizzare l'efficacia complessiva dell'azione di governo.

Al netto delle varie e diverse declinazioni, i CSN sono organi di raccordo in cui sono rappresentati gli stakeholder della sicurezza nazionale. Questi includono sempre Ministeri, Agenzie e altri organi dello Stato competenti e talvolta, in formato temporaneo e

variabile a seconda dei temi trattati, compagnie private di interesse pubblico o altri ancora. La produzione del CSN consiste in analisi delle minacce alla sicurezza e relative proposte e raccomandazioni di policy all'indirizzo del Vertice del Governo.

Le caratteristiche dei CSN istituiti dagli Alleati rispecchiano le rispettive sensibilità e architetture istituzionali e non possono essere automaticamente trasposti nel contesto italiano. Si possono tuttavia isolare tre caratteristiche che ricorrono nelle esperienze più riuscite e che potrebbero essere replicate in un ipotetico CSN nazionale. In particolare, quest'ultimo dovrebbe essere:

a. **Permanente**: per fare fronte alla sfida descritta finora, il CSN NON dovrebbe essere un organo di crisi. Al contrario, in linea con il suo compito strategico, dovrebbe costituirsi come un organo permanente e garantire una calibrazione costante, quotidiana della policy di governo;

b. **Tecnico**: a corollario del punto precedente, è fondamentale che gli stakeholder rappresentati nel CSN non siano rappresentati unicamente a livello di vertice. Beninteso, un formato a livello politico è perfettamente logico e previsto in tutti i CSN degli Alleati. Tuttavia, è imprescindibile che il CSN sia primariamente un organo tecnico e che si avvalga di personale a impiego permanente, per garantire l'expertise e il focus necessari allo svolgimento della sua funzione. Ciò potrebbe essere realizzato attraverso un segretariato permanente incardinato presso la Presidenza del Consiglio e composto di personale di medio livello, assunto dall'esterno o distaccato dalle altre amministrazioni dello Stato. Lo staff avrebbe anche il compito di raccordarsi con esse e definire di conseguenza l'ordine del giorno del CSN.

c. **Dipendente dal Presidente del Consiglio**: il CSN dovrebbe essere guidato da una figura di diretta nomina ed emanazione del Presidente del Consiglio, investita dell'autorità per gerarchizzare e conciliare le priorità delle diverse amministrazioni in una politica di sicurezza armonica. Inoltre, la guida del CSN non dovrebbe fare parte di una delle amministrazioni che lo compongono. Oltre a essere una garanzia di imparzialità, ciò rispecchia la necessità di rafforzare un concetto di sicurezza nazionale completo e non appiattito su una delle sue dimensioni (diplomatica, militare, economica ecc.).

Infine, l'operato dei CSN si impernia solitamente su una strategia di sicurezza nazionale, che spesso formula esso stesso e di cui valuta l'esecuzione. Senza entrare nella legittima questione su cosa debba venire prima fra una strategia di sicurezza nazionale e un CSN, è sufficiente osservare come, dopo la recente pubblicazione (14 giugno 2023) della prima strategia di sicurezza nazionale tedesca, l'Italia sia rimasta l'unico Paese membro del G7 a non esserne dotata.

Il ritorno della guerra in Europa, la continua pressione migratoria dalla nostra periferia meridionale e il nuovo focolaio mediorientale sono solo alcuni esempi di tempeste che, oltre a portare minacce immediate e tangibili, distolgono lo sguardo dall'orizzonte strategico. Lungi dall'allontanare il "climate change", la distrazione dell'attenzione e delle risorse dalle minacce di più lungo periodo le accelera, a vantaggio dei loro originatori. Da qui l'urgenza di individuare un organismo deputato a vigilare sulla dimensione sistemica delle minacce, contribuendo alla resilienza complessiva del Paese anche rispetto alle singole tempeste.