Atti di convegno

L'epoca delle guerre ibride e le nuove frontiere delle attività di intelligence

Mario Schirripa
Ricercatore - Università degli Studi 'Mediterranea' di Reggio Calabria

"The age of hybrid warfare and the new frontiers of intelligence activities"

Abstract

2023 Report on Information Policy for Security highlights that cyber and hybrid threats are becoming increasingly dangerous for the stability of both European and national security, requiring targeted strategies and international cooperation. The complexity of the issue calls for a new security culture that integrates technological, regulatory, and intelligence tools. Intelligence is playing an increasingly central role in defending democracies and the rule of law. Not by chance, even in Italy, legislation is assigning increasingly significant responsibilities to the intelligence sector to safeguard the salus rei publicae.

Keywords: Hybrid warfare - Disinformation - Intelligence - Cybersecurity - Cooperation

1. Le nuove guerre ibride tra disinformazione e attacchi cibernetici

Dalla lettura dell'ultima 'Relazione sulla politica dell'informazione per la sicurezza' relativa all'operato di DIS (Dipartimento delle informazioni per la sicurezza), AISI (Agenzia informazioni e sicurezza interna) e AISE (Agenzia informazioni e sicurezza esterna) nel 2023, emerge che saremo «chiamati ogni giorno di più a confrontarci con minacce cyber e ibride, comprese le campagne di disinformazione, e l'uso dannoso di tecnologie emergenti sempre più sofisticate, come l'intelligenza artificiale, per fini malevoli»[1].

La sicurezza cibernetica ha costituito oggetto di approfondimento anche da parte del COPASIR (Comitato parlamentare per la sicurezza della Repubblica) nell'ambito di diverse audizioni e all'interno delle relazioni annuali sulle attività svolte[2], ad ulteriore riprova dell'accresciuta esposizione di molteplici settori ad attacchi e minacce a livello globale. Emerge, dunque, che il campo di battaglia non è più solo quello fisico[3], fatto di carrarmati, droni, armi e militari, ma è sempre più quello virtuale, che sfrutta le tecnologie più progredite per colpire "in silenzio" il nemico, attraverso lo spionaggio, la propaganda, la disinformazione e/o l'attacco informatico, penetrando nelle sue strutture interne e strategiche[4].

Ci si trova dinanzi ad un nuovo equilibrio geopolitico, all'interno del quale il ruolo di uno Stato nella competizione globale è definito più dal livello di innovazione tecnologica che dalla potenza militare ed economica in quanto tali, poiché queste ultime due variabili dipendono ormai dalla prima[5]. In questo scenario, le guerre contemporanee assumono una forma ibrida[6], pianificata ed alimentata dalla disinformazione, dalla produzione sistematica di false notizie e da attacchi cibernetici[7].

---

[1] La Relazione è disponibile al link https://www.sicurezzanazionale.gov.it/data/cms/posts/933/attachments/711cf87b-1a38-4864-975a-e253a67cbdba/download?view=true. Il passaggio riportato si trova a p.52.

Per un commento sulla Relazione, si consiglia la lettura di M. Santarelli, Relazione Intelligence 2023: la risposta dell'Italia a minacce ibride e conflitti globali, in www.agendadigitale.eu, 7 marzo 2024.

[2] Per un approfondimento vd. Relazione del Copasir sull'attività svolta dal 6 dicembre 2022 al 31 dicembre 2023 su https://parlamento18.camera.it/228.

[3] Per una riflessione su come sia, nel tempo, evoluto il concetto di guerra vd. G. de Vergottini, Guerra e costituzione. Nuovi conflitti e sfide alla democrazia, il Mulino, 2004; A. Vedaschi, À la guerre comme à la guerre. La disciplina della guerra nel diritto costituzionale comparato, Torino, 2007.

[4] I settori più colpiti sono le filiere delle infrastrutture digitali/servizi IT, dell'energia, dei trasporti e il settore pubblico-istituzionale.

[5] Così A. Pagani, La guerra cibernetica nell'età ibrida: tecnologie, strategie e priorità, in www.agendadigitale.eu, 22 luglio 2021.

[6] Sul concetto di guerra ibrida si veda il recente contributo di C. Sbailò, Guerre ibride: quali risposte possibili?, in DPCE online, vol. 63, no. SP1, 2024.

[7] Vd., in proposito, A. Spaziani, L'attacco cibernetico nell'era della guerra ibrida, in DPCE online, vol. 63, no. SP1, 2024 e F. Nisticò, L'elemento cyber nella guerra russo-ucraina, in aspeniaonline.it, 3 marzo 2022.

L'ingerenza sempre maggiore delle nuove tecnologie nelle guerre di oggi ha portato a coniare nuovi termini quali information warfare[8], cyberwarfare[9], electronic warfare[10], psychological warfare[11], hacker warfare[12], economic information warfare[13], tutte diverse declinazioni della hybrid warfare.

Se ci si sofferma sull'impiego della disinformazione come arma, il conflitto russo-ucraino ne rappresenta un esempio perfetto sin dal suo inizio quando, il 22 febbraio 2022, il presidente Putin definì «operazione militare speciale»[14] quella che, di fatto, è stata l'invasione di uno Stato sovrano, una guerra a tutti gli effetti. Sin dal principio, quindi, il tentativo di condizionare l'opinione pubblica è stato imponente e senza precedenti. È stata scientificamente architettata una campagna di disinformazione con diffusione di fake news frutto di una strategia ben congegnata[15].

Sia chiaro, concetti come 'disinformazione' e 'guerra ibrida' non nascono certo oggi. Si possono trovare degli esempi che risalgono alla storia dei tempi: dal famoso mito del cavallo di Troia al celebre trattato di strategia militare di Sun Tzu, L'arte della guerra, in cui l'autore sosteneva che «l'inganno è il Tao della Guerra».

Quello che cambia significativamente nell'epoca attuale è il grado di penetrazione delle tecnologie in ogni ambito dell'esistenza, il loro grado di pervasività e di diffusione che mette fuori gioco gran parte delle norme[16].

---

[8] La guerra spostata sui media, che pone al centro della sua attenzione l'informazione e il cui obiettivo è quello di ottenere un vantaggio informativo sull'avversario. Può dirsi che si tratta di una tecnica di conflitto che trasforma i mezzi di informazione in armi che entrano a pieno titolo nel campo di battaglia. Sull'evoluzione dell'Information Warfare si veda M.C. Libicki, The Convergence of Information Warfare, in Strategic Studies Quarterly, Volume 11, Issue 1, 2017, pp.49-65.

[9] Ovvero l'attività e la modalità di combattimento attraverso gli strumenti informatici volta a manipolare o distruggere i sistemi informativi per scopi strategici, politici o militari.

[10] Che impiega strumenti radio, elettronici e crittografici.

[11] Che mira ad influenzare le opinioni di persone e comunità attraverso le PSYOP(psychological operations).

[12] Riguarda gli attacchi alle reti telematiche.

[13] Attiene alla sicurezza e agli interessi economici nazionali.

[14] Sul punto, si consiglia la lettura di I. Galimova, L'"operazione militare speciale" in Ucraina e la reazione del sistema politico russo, in Nomos. Le attualità del diritto, n.1, 2022 (https://www.nomos-leattualitaneldiritto.it/wp-content/uploads/2022/06/RUSSIA-1_2022formattato.pdf)

[15] Sul tema della disinformazione si veda, ex multis, M. Caligiuri, A. Pagani, M. Chioso, Disinformare: ecco l'arma. L'emergenza educativa e democratica del nostro tempo, Rubbettino, 2024; S. Sassi, Disinformazione contro Costituzionalismo, Editoriale Scientifica, Napoli, 2021;A. Alù, Perché la disinformazione minaccia le democrazie nel 2024, in agendadigitale.eu, 7 febbraio 2024; M. Caligiuri, Come i pesci nell'acqua. Immersi nella disinformazione, Rubbettino, Soveria Mannelli, 2019; G. Pitruzzella, O. Pollicino, Disinformation and Hate Speech. A European Constitutional Perspective, Egea, Milano, 2020; C. Pinelli, C. Hassan, Disinformazione e democrazia, Marsilio Editori, 2022.

[16] Cfr. H. Kissinger, Ordine Mondiale, Mondadori, 2017, p.339.

L'arma della disinformazione implica effetti sotto diversi profili: sociali, economici e culturali. Basti pensare al fenomeno della polarizzazione creato dalle cd. echo chambers (bolle informative chiuse); alla sfiducia nelle istituzioni; alle campagne mirate su cleavages identitari; agli effetti della manipolazione informativa sui mercati (vendite, brand, indici di borsa); alle campagne sul revisionismo storico; allo sfruttamento delle fratture sociali (migrazioni, minoranze, diritti); al tentativo di alterare gli esiti delle elezioni politiche, come sembrerebbe sia avvenuto in Romania nel 2024[17].

Per contrastare tali minacce, la Svezia, sin dal 2022, si è dotata della Psychological Defence Agency, un'agenzia governativa che ha il compito di «identify, analyse and provide support in countering malign information influence and other misleading information that is directed at Sweden or Swedish interests by antagonistic foreign powers. This can concern disinformation aimed at weakening Sweden's resilience and the willingness of the population to defend itself, or unduly influencing people's perceptions, behaviours and decision-making»[18], ad ulteriore riprova che la sicurezza nazionale di un Paese dipende, ormai, anche dalla sua capacità di risposta alle insidie della disinformazione e degli attacchi informatici.

Nell'ambito dello spionaggio informatico, tali attacchi sono realizzati da attori statuali denominati Advanced Persistent Threat (APT) una tipologia di attacchi mirati e persistenti con tecniche hacking avanzate[19]. Attribuire un attacco informatico ad un gruppo ATP è un'operazione complessa e di difficile realizzazione, tuttavia alcuni di essi diventano inevitabilmente di pubblico dominio in conseguenza dei loro effetti esterni. Si pensi al virus Stuxnet, il primo malware della guerra cyber, creato nel 2010 da Usa e Israele per bloccare il programma nucleare iraniano. È considerato il primo atto di cyberwar al mondo e all'epoca compromise il sistema di controllo automatico delle centrifughe in un sito iraniano di arricchimento dell'uranio, mettendo in risalto in modo clamoroso la vulnerabilità degli impianti industriali agli attacchi cibernetici. Ancora più sconcertante fu scoprire che l'episodio era stato provocato da una semplice pen drive USB infetta, estendendo così la portata della minaccia all'intero settore industriale globale.

Rispetto alle cd. guerre convenzionali, l'hybrid warfare si caratterizza per la sua ambiguità, poiché l'attribuzione degli attacchi è spesso incerta, creando difficoltà nelle risposte politiche e strategiche; per l'incertezza degli effetti, poiché gli attacchi informatici possono assumere esiti imprevedibili; per la capacità di persistenza, poiché le operazioni cibernetiche possono essere condotte senza interruzioni, a differenza dei conflitti cinetici.

---

[17] Per un approfondimento si rimanda a F. Rosa, L'annullamento delle elezioni presidenziali in Romania e la difficile difesa della democrazia, in Federalismi.it, n.15, 2025, pp. 53-75.

[18] Vd. https://mpf.se/psychological-defence-agency/about-us/our-mission.

[19] Sul punto si veda R. Baldoni, Sovranità digitale. Cos'è e quali sono le principali minacce al cyberspazio nazionale, Il Mulino, Bologna, 2025, p. 61 e ss.

Ad oggi, non esiste un solo settore impermeabile al cyber space: servizi economici e finanziari, sistemi di comando e controllo militare, sistemi di fornitura di energia elettrica o acqua, l'assistenza sanitaria, le telecomunicazioni, dispositivi fisici con cui si interagisce giornalmente, sono tutti controllati da sistemi informatici. La complessità della questione necessita di una nuova cultura della sicurezza che coinvolga strumenti tecnologici, normativi e di intelligence. Quest'ultima assume un ruolo sempre più centrale per la difesa delle democrazie e dello Stato di diritto, non a caso, anche in Italia, per legge, si stanno assegnando compiti sempre più rilevanti al comparto intelligence per affrontare le nuove sfide della sicurezza informatica[20].

2. Il ruolo guida dell'Agenzia per la Cybersicurezza Nazionale italiana

Con l'adozione del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, è stata istituita l'Agenzia per la cyber sicurezza nazionale (ACN), la cui missione istituzionale è quella di potenziare la resilienza cibernetica del Paese[21], riducendone il grado di vulnerabilità e incrementandone l'autonomia e l'indipendenza tecnologica, con la finalità di assicurare una maggiore competitività nello scenario internazionale laddove le operazioni di cyber-intelligence rimangono di esclusiva e peculiare competenza del Comparto informativo[22]. Si è, così, colmata una importante lacuna[23] che l'Italia scontava da decenni, soprattutto se posta a confronto con i maggiori partner europei[24].

Va segnalato che il percorso che ha condotto alla stesura del testo normativo che ha definito le competenze dell'ACN e ridisegnato l'architettura di cybersicurezza nazionale, ha registrato il coinvolgimento del COPASIR fin dalle prime fasi. Tale coinvolgimento

---

[20]Ex plurimis, si veda C. Mosca, Democrazia e intelligence italiana. Dieci anni dopo tra cultura, diritto e nuove sfide della democrazia, Editoriale scientifica, 2018, pp. 161-197; M. Caligiuri, Cyber intelligence. Tra libertà e sicurezza, Donzelli, 2016.

[21] Sull'attività dell'ACN ed il suo obiettivo di accompagnare una trasformazione digitale in sicurezza per la prosperità e l'indipendenza dell'Italia, vd. R. Baldoni, Così l'Agenzia cyber sta lavorando e dispiega i propri effetti, in agendadigitale.eu, 18 novembre 2021 (https://www.agendadigitale.eu/sicurezza/baldoni-cosi-lagenzia-cyber-sta-lavorando-e-dispiega-i-propri-effetti/).

[22]L'istituzione dell'Agenzia per la Cybersicurezza Nazionale è ritenuta uno snodo fondamentale nell'architettura generale dell'intelligence nella "Relazione sulla politica dell'informazione per la sicurezza" relativa all'anno 2021, curata dal Comparto Intelligence, ai sensi della quale il Governo riferisce ogni anno al Parlamento con una Relazione non classificata sulla politica dell'informazione per la sicurezza (https://www.sicurezzanazionale.gov.it/sisr.nsf/relazione-annuale/relazione-al-parlamento-2021.html). Si veda anche la Relazione del Copasir sull'attività svolta dal 1° gennaio 2021 al 9 febbraio 2022, pp. 35-37 e 100-101 (https://www.senato.it/service/PDF/PDFServer/BGT/1332539.pdf).

[23] L'Italia si trova costantemente esposta ad attacchi cibernetici, in taluni casi anche con effetti di notevole ampiezza e gravità. Si pensi ad esempio al caso dell'attacco sferrato alla fine del mese di luglio del 2021 nei confronti dei sistemi informatici della Regione Lazio e le conseguenti ricadute sulle attività e i servizi erogati dalla Regione stessa, compresi quelli connessi con il Sistema sanitario regionale in un periodo particolarmente critico come quello che stiamo vivendo a causa della pandemia da SARS-CoV-2.

[24] Per un confronto tra l'Agenzia per la cybersicurezza nazionale e gli omologhi organismi europei, vd. M. Artini, Agenzia Cibernetica Nazionale italiana, confrontiamola con gli altri attori europei, in agendadigitale.eu, 17 gennaio 2022 (https://www.agendadigitale.eu/sicurezza/lagenzia-cibernetica-nazionale-italiana-il-confronto-con-gli-altri-attori-europei/).

è apparso naturale se si considera che all'agenzia sono state trasferite anche le competenze sulla resilienza in ambito cibernetico fino ad allora affidate al Dipartimento delle informazioni per la sicurezza (DIS). Il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, attribuisce al Copasir alcune specifiche competenze ricalcando sostanzialmente quanto previsto dalla legge n. 124 del 2007 nell'ambito del Sistema di informazione per la sicurezza della Repubblica. Il Presidente del Consiglio e l'ACN sono sottoposti, infatti, ad una serie di oneri informativi che hanno come destinatari il Copasir e le Commissioni parlamentari competenti. In primo luogo, il Presidente del Consiglio dei ministri informa preventivamente tali destinatari sulle nomine del direttore e del vice direttore dell'Agenzia (articolo 2, comma 3). Inoltre, l'Agenzia invia al Copasir e alle Commissioni competenti il bilancio consuntivo accompagnato dalla relazione della Corte dei conti (articolo 11, comma 3) e dà tempestiva e motivata comunicazione dei provvedimenti adottati in materia di dotazione organica (articolo 12, comma 5). Vi sono poi ulteriori oneri informativi riguardanti unicamente il Copasir che viene informato da parte del Presidente del Consiglio sulla determinazione del fabbisogno annuo dell'Agenzia (articolo 11, comma 1) e riceve, entro il 30 giugno di ogni anno, la relazione sulle attività dell'Agenzia negli ambiti concernenti la tutela della sicurezza nazionale nello spazio cibernetico, relativamente ai profili di competenza del Copasir (articolo 14, comma 2). Infine, il Presidente del Consiglio informa il Comitato sulle spese per la prima operatività dell'Agenzia fino all'adozione dei regolamenti di contabilità e su appalti e forniture (articolo 17, comma 7). L'Agenzia, inoltre, costituisce l'organismo che, per l'Italia, terrà le relazioni con il Centro di competenza europeo in cybersecurity (ECCC). Tale organismo, con sede a Bucarest, collaborando con la rete dei centri nazionali di coordinamento designati dagli Stati membri, aiuterà l'Unione europea ad aggregare e collegare in rete le sue competenze nello sviluppo industriale, nella tecnologia e nella ricerca sulla cyber sicurezza e a promuovere la diffusione delle soluzioni più recenti nel campo della sicurezza informatica. Pur osservando che il citato decreto-legge 14 giugno 2021, n. 82, non interviene sulla legge 3 agosto 2007, n. 124, è evidente la stretta interconnessione determinata dal fatto che la sicurezza cibernetica è una sfera sempre più rilevante della sicurezza nazionale. Il coordinamento tra il comparto dell'intelligence e l'Agenzia per la cybersicurezza nazionale risulta, dunque, fondamentale. Può dirsi che all'ACN spettino le attività di prevenzione e mitigazione degli attacchi cibernetici, mentre gli interventi di reazione e di contrasto a questi ultimi competono agli apparati di intelligence. Tali aspetti andrebbero definiti con una revisione della legge n. 124, al fine di armonizzare le nuove disposizioni di legge relative all'ACN, delineare i perimetri di competenza ed evitare sovrapposizioni[25].

---

[25] Sul dibattito, sempre più attuale, relativo all'aggiornamento della l.124 del 2007 vd. A. Monti, Il rinnovamento dell'intelligence ha bisogno di coerenza normativa, in formiche.net, 6 dicembre 2020 (https://formiche.net/2020/12/il-rinnovamento-dellintelligence-ha-bisogno-di-coerenza-normativa/); G. Carrer, Riforma dell'intelligence? Sì, dicono Pagani (Pd), Perego (FI) e Tofalo (M5S), in formiche.net, 29 luglio 2021 (https://formiche.net/2021/07/riforma-intelligence-pagani-perego-tofalo/); U. Saccone, Quale Intelligence per il futuro?, in formiche.net, 2 agosto 2021 (https://formiche.net/2021/08/riforma-intelligence-

2.1 Le attività svolte dall'ACN e la Direttiva NIS 2

Per misurare lo stato di salute della sicurezza cibernetica in Italia risultano preziose le relazioni annuali sulle attività svolte dall'ACN, in cui vengono illustrate le minacce affrontate, le azioni intraprese e le strategie per migliorare la resilienza digitale del Paese[26]. Il 2023 è stato caratterizzato da un aumento significativo delle aggressioni cibernetiche, spesso collegate a conflitti internazionali (si pensi, in particolare, a quanto accade in Ucraina e Medio Oriente). Uno dei pilastri su cui regge l'attività dell'ACN è rappresentato dal Computer Security Incident Response Team (CSIRT), l'organo dell'Agenzia per la cybersicurezza nazionale che si occupa di monitoraggio preventivo e risposta agli incidenti informatici. Il CSIRT Italia, solamente nel 2023, ha monitorato e gestito oltre 1.400 eventi cyber - con un aumento del 30% rispetto al 2022 - di questi, 303 sono stati classificati come incidenti, per una media di circa 25 al mese, più che raddoppiati rispetto all'anno precedente. Gli attacchi DDoS[27] sono aumentati del 625%, molti dei quali legati al cyber-attivismo filo-russo e filo-palestinese. Il ransomware[28] rimane la minaccia più grave, con un incremento del 27% rispetto al 2022, che ha portatol'Italia ad essere il terzo Paese dell'Unione europea più colpito da ransomware nel 2023 ed il sesto a livello globale[29]. Come se non bastasse, sempre nel solo 2023, sono stati segnalati 584 tentativi di phishing[30]e analizzati 100 malware[31]. Sono numeri impietosi che hanno condotto, sul piano normativo, all'implementazione della Direttiva NIS 2[32] per rafforzare la sicurezza delle reti e sistemi

---

umberto-saccone-ifi/); F. Bechis, Non solo cyber, così riformiamo l'intelligence. Parla Franco Gabrielli, in formiche.net, 14 agosto 2021 (https://formiche.net/2021/08/non-solo-cyber-cosi-riformiamo-lintelligence-parla-franco-gabrielli/).

[26] Vd. Relazione annuale al Parlamento dell'ACN del 2023 e del 2022, entrambe consultabili al seguente link https://www.acn.gov.it/portale/relazione-annuale. Sull'importanza dell'attività svolta dall'ACN si legga R. Baldoni, Il ruolo guida dell'Agenzia per la Cybersicurezza Nazionale (ACN) verso la Cyber-Resilienza Nazionale: sinergie pubblico-private, in U. Gori (a cura di), Cyber Warfare 2021-2022. Cibersicurezza: dalla collaborazione Pubblico-Privato alla difesa dello Stato, Franco Angeli, 2023, pp. 21-25.

[27] Gli eventi DDoS (Distributed Denial of Service) mirano a compromettere la disponibilità di un sistema mediante esaurimento delle sue risorse di rete, elaborazione o memoria. L'effetto più immediato di tale tipologia di attacco è l'indisponibilità del sito o del servizio colpito.

[28] In questo tipo di minaccia l'attaccante, di regola, si introduce nei sistemi di un privato o di un'organizzazione per cifrarne i dati, al fine di ottenere il pagamento di un riscatto per rendere nuovamente disponibili i dati al legittimo proprietario e/o non diffonderli pubblicamente.

[29] Sui numeri del CSIRT Italia vd. Relazione annuale al Parlamento dell'ACN del 2023, pp. 9-20.

[30] Attacco informatico avente, generalmente, l'obiettivo di carpire informazioni sensibili (user ID, password, numeri di carte di credito, PIN) con l'invio di false e-mail generiche a un gran numero di indirizzi. Le e-mail sono congegnate per convincere i destinatari ad aprire un allegato o ad accedere a siti web fake. L'attaccante utilizza i dati carpiti per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

[31] Programma inserito in un sistema informatico, generalmente in modo abusivo e occulto, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo.

[32] La Direttiva NIS 2 (Direttiva UE 2022/2555) supera e rafforza l'impianto normativo previsto dalla precedente Direttiva NIS (Direttiva (UE) 2016/1148), facendo tesoro dell'esperienza acquisita nella sua applicazione.

informativi essenziali. La nuova direttiva amplia il numero di settori e soggetti obbligati ad adottare misure di cybersicurezza, includendo settori come energia, trasporti, sanità, servizi finanziari e pubblica amministrazione e l'ACN è coinvolta nell'attuazione normativa e nel monitoraggio dell'adeguamento delle aziende e delle amministrazioni pubbliche.

Le principali novità introdotte dalla Direttiva NIS 2 consistono: nell'espansione del perimetro di applicazione (mentre la prima NIS si applicava solo agli "Operatori di Servizi Essenziali" e ai "Fornitori di Servizi Digitali", la NIS 2 include nuove categorie di soggetti, come enti pubblici e aziende di rilevanza economica); in obblighi più stringenti per la gestione del rischio (i soggetti coinvolti devono implementare misure avanzate di sicurezza, come i sistemi di gestione del rischio basati su valutazioni periodiche delle vulnerabilità, i piani di gestione degli incidenti con una chiara definizione delle responsabilità, le misure di prevenzione e risposta contro attacchi cyber); in una maggior cooperazione tra Stati membri (la NIS 2 rafforza i meccanismi di scambio di informazioni tra le autorità nazionali ed europee in caso di crisi cibernetiche); nell'introduzione di sanzioni (i soggetti che non rispettano gli obblighi di sicurezza possono essere sanzionati con multe proporzionali alla gravità della violazione).

La Direttiva NIS 2 rappresenta, dunque, un cambiamento radicale nel quadro normativo europeo sulla cybersicurezza ed una sfida per le infrastrutture critiche italiane, che devono adeguarsi a standard più elevati in termini di sicurezza cibernetica.

In questo processo, sarà compito dell'ACN quello di garantire il coordinamento nazionale, supportare il recepimento della normativa e assistere i soggetti interessati[33].

3. Uno sguardo comparato alle agenzie di cybersicurezza europee

Allargando lo sguardo al di là dei confini nazionali, una breve analisi delle esperienze di Francia, Regno Unito e Spagna può contribuire a comprendere la grande rilevanza che il tema della cyber intelligence ricopre anche all'estero. In Francia, un ruolo fondamentale è svolto dall'Agenzia nazionale della sicurezza dei sistemi di informazione (Agence Nationale de la Sécurité des Systèmes d'Information, ANSSI), che è il principale soggetto incaricato di misurare e valutare i rischi e gli effetti degli attacchi informatici, rivolti sia ai soggetti pubblici sia ai privati.

---

[33] A tal proposito il Servizio Operazioni e gestione delle crisi cyber di ACN, il 22 febbraio 2025, ha pubblicato un rapporto sulla minaccia Denial of Service (DoS) e Distributed Denial of Service (DDoS), analizzando le strategie d'attacco più diffuse e fornendo raccomandazioni specifiche per la mitigazione del rischio. Per consultare il rapporto vd. https://www.acn.gov.it/portale/w/acn-pubblica-il-rapporto-sugli-attacchi-ddos.

Il ruolo dell'ANSSI è quello di promuovere una risposta coordinata ed efficiente ai problemi di della sicurezza digitale in Francia. L'Agenzia, istituita con il Décret n. 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé «Agence nationale de la sécurité des systèmes d'information», svolge in particolare le seguenti funzioni: assicura la funzione di autorità nazionale per la difesa dei sistemi di informazione e, in questa veste, propone al Primo ministro misure per rispondere alle crisi che incidono o minacciano la sicurezza dei sistemi di informazione delle autorità pubbliche; progetta, fa realizzare e attua i mezzi interministeriali sicuri di comunicazioni elettroniche necessari per il Presidente della Repubblica e il Governo; anima e coordina i lavori interministeriali sulla sicurezza dei sistemi informativi; elabora le misure di protezione dei sistemi di informazione proposti al Primo ministro; assicura l'applicazione delle misure adottate; effettua ispezioni dei sistemi informativi dei servizi statali e degli operatori pubblici o privati[34].

L'ANSSI fa riferimento al Segretario della difesa e della sicurezza nazionale (Secrétaire général de la défense et de la sécurité nationale), che assiste il Primo ministro nell'esercizio delle sue responsabilità in materia di difesa e sicurezza. La Direzione dell'ANSSI è affidata a un Direttore generale, nominato dal Primo ministro. Così come in Francia, nel Regno Unito il tema della sicurezza delle infrastrutture di interesse nazionale (critical national infrastructures – CNI) e della loro esposizione al rischio di attacchi cibernetici è stato oggetto, negli ultimi anni, di specifiche iniziative del Governo e del Parlamento.

Significative innovazioni in materia di cybersicurezza si correlano all'adozione, nel 2016, del pioneristico piano strategico nazionale quinquennale ad essa specificamente dedicato (National Cyber Security Strategy 2016-2021 - NCSS, dotata di uno stanziamento di 1,9 miliardi di sterline) ed alla più recente Government Cyber Security Strategy 2022–2030[35]. In particolare, si è provveduto ad istituire un organismo tecnico ad hoc, il National Cyber Security Centre (NCSC), preposto alla gestione degli incidenti di rilievo nazionale nel campo della cibersicurezza e all'assistenza tecnica diretta ai dipartimenti governativi, alle amministrazioni pubbliche e alle imprese attraverso attività di analisi e di individuazione delle minacce, di consulenza, di promozione dell'innovazione e delle competenze professionali in materia. Il National Cyber Security Center è divenuto, così, il braccio per la sicurezza informatica del Government Communications Headquarters (GCHQ)[36], l'agenzia di intelligence britannica nata come British Signals Intelligence nell'agosto del 1914[37], durante la Prima Guerra Mondiale, al fine di istituire un organo deputato all'intercettazione e

[34] Per un approfondimento sulla normativa relativa all'ANSSI, vd. https://cyber.gouv.fr/sinformer-sur-la-reglementation.

[35] Per la lettura della nuova strategia nazionale per la sicurezza informatica del Regno Unito si rimanda al seguente link https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022.

[36] Il Government Communications Headquarters ha sede a Cheltenham e l'attuale Direttore è Jeremy Fleming. Il suo sito ufficiale è https://www.gchq.gov.uk/.

[37] Per un approfondimento sulla storia del GCHQ cfr. https://www.gchq.gov.uk/section/history/our-origins-and-wwi. Alastair Denniston è stato il primo capo del GCHQ in servizio dal 1919 al 1942.

decriptazione dei messaggi radio delle forze nemiche. Il GCHQ è specializzato nell'utilizzo delle nuove tecnologie e le sue mission areas sono: Counter Terrorism, la Cyber Security, Strategic Advantage, Serious and Organised Crime, Support to Defence[38]. Il suo ruolo principale consiste nell'assicurare assistenza e consulenza ai Dipartimenti Governativi e alle Forze Armate sulla sicurezza delle loro comunicazioni e informazioni sui sistemi tecnologici.

Anche la Spagna, sin dal 2004, si è dotata di un apposito organismo di cybersicurezza per far fronte alle nuove minacce informatiche. Si tratta del Centro Criptológico Nacional (CCN) istituito con il Real Decreto 421/2004 e connesso al Centro Nacional de Inteligencia (CNI), l'agenzia di intelligence ufficiale spagnola che si occupa sia della sicurezza estera che di quella nazionale. La Ley 11/2002[39], che delinea il quadro normativo dell'intelligence spagnola, affida al Centro Nacional de Inteligencia l'esercizio delle funzioni relative alla sicurezza delle tecnologie informatiche all'articolo 4 lett. e)[40] e, allo stesso tempo, conferisce al suo Direttore la responsabilità di dirigere il Centro Criptológico Nacional all'articolo 9 comma 2 lett. f)[41]. Per questo motivo, il CCN condivide mezzi, procedure, regolamenti e risorse con il CNI. Tra i principali compiti del CCN si annoverano lo sviluppo e la diffusione di standard, istruzioni, guide e raccomandazioni per garantire la sicurezza dei sistemi ICT (Information and Communication Technologies) e il rispetto delle normative relative alla protezione delle informazioni classificate nel proprio ambito di competenza.

4. Verso una nuova cultura della sicurezza europea e nazionale

Alla luce di quanto esposto, emerge come negli ultimi anni la materia della sicurezza informatica e della cyber intelligence abbia assunto un interesse sempre più crescente sia in ambito nazionale che europeo. Ciò rappresenta l'esito di una maggiore consapevolezza che è maturata attorno al tema a causa dell'innegabile e notevole incremento – sia in termini di numeri che di complessità – degli attacchi cyber rilevati. Tale consapevolezza si è tradotta in interventi volti a costruire un'elevata protezione dello Stato sotto il versante digitale. È nata perciò la necessità di dare una nuova forma alla difesa degli interessi strategici nazionali e di investire in maniera robusta nel campo della cyber intelligence anche tramite la creazione di agenzie

[38] Cfr. https://www.gchq.gov.uk/.

[39] Per visionare il testo completo della legge si rimanda a https://www.boe.es/buscar/act.php?id=BOE-A-2002-8628.

[40]Artículo 4. Funciones del Centro Nacional de Inteligencia. Para el cumplimiento de sus objetivos, el Centro Nacional de Inteligencia llevará a cabo las siguientes funciones: [...] e) Coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada de material criptológico y formar al personal, propio o de otros servicios de la Administración, especialista en este campo para asegurar el adecuado cumplimiento de las misiones del Centro.

[41]Artículo 9.2. Corresponde al Secretario de Estado Director del Centro Nacional de Inteligencia impulsar la actuación del Centro y coordinar sus unidades para la consecución de los objetivos de inteligencia fijados por el Gobierno, asegurar la adecuación de las actividades del Centro a dichos objetivos y ostentar la representación de aquél. Asimismo, le corresponde: [...] f) Desempeñar las funciones de Autoridad Nacional de Inteligencia y Contrainteligencia y la dirección del Centro Criptológico Nacional.

specializzate.

Le guerre contemporanee assumono una natura sempre più economica e digitale e vengono combattute sul web a colpi di algoritmi. Le armi sono sostituite dalle attività di informazione/disinformazione e le sanzioni dei Mercati spesso spaventano più di quelle degli Stati. In un quadro di tal genere, le nuove frontiere delle attività di intelligence non possono che riguardare il campo della cybersecurity e dell'intelligence finanziaria e necessitano di una cooperazione internazionale più robusta di quella attuale, proprio per la natura sovranazionale delle minacce da affrontare. Va detto che, da anni, è in corso un lento ma costante processo di cooperazione tra Stati europei nel campo dell'intelligence, che ha portato alla creazione di organismi di coordinamento fra i maggiori servizi di sicurezza e d'informazione come, ad esempio, il Club di Berna[42]. Ad oggi, la rete transnazionale di intelligence che più si avvicina alla cooperazione strutturata europea[43] è rappresentata dall' EU Intelligence and Situation Centre (EU IntCen). Va, però, sottolineato che nel lavoro condotto dall'EU IntCen, sono sempre i singoli Stati a decidere quali informazioni sulla sicurezza condividere (la sicurezza nazionale è di esclusiva responsabilità di ciascuno Stato membro), non l'Unione europea nella sua interezza. L'EU IntCen non è, dunque, una agenzia di intelligence europea strutturata ma è certamente ciò che più si avvicina ad essa, poiché svolge un ruolo da protagonista nel coordinamento della cooperazione di intelligence[44] e ha assunto un ruolo crescente nella politica estera europea.

Appare evidente, dunque, che un sistema di cooperazione di intelligence europea esiste, seppur non strutturato e non integrato alle istituzioni europee e basato su una condivisione di informazioni volontaria.

Un eventuale passo in avanti per la creazione di una Agenzia di intelligence europea presenta una serie di ostacoli di non poco conto. La prima, evidente, complicazione risiede nel fatto che l'attività di intelligence rappresenta, da sempre, il cuore dello Stato nazione ed una roccaforte della sovranità nazionale. Vi è, poi, da parte dei servizi di sicurezza nazionali, il timore di diffondere fonti riservate e relazioni privilegiate, soprattutto se riguardanti aree di competizione tra Stati, come ad esempio l'ambito industriale o commerciale. Non è un mistero che, soprattutto nel campo del mercato economico, alcune fonti siano preziose ed assicurino vantaggi competitivi solo a patto che siano conosciute da un solo attore.

---

[42] Oltre al Club di Berna, un altro esempio di cooperazione non strutturata di servizi di intelligence è il cosiddetto gruppo Kilowatt. Questa alleanza informativa tra i servizi di circa 15 paesi, risalente al 1977, è stata tenuta a lungo segreta. Nel 1982, la sua esistenza è stata rivelata quando sono stati scoperti alcuni documenti, presso l'ambasciata americana di Teheran, in cui veniva menzionata. Alla rete Kilowatt partecipano i paesi della comunità europea, il Canada, la Norvegia, la Svezia, la Svizzera, la CIA, l'FBI, il Mossad e lo Shin Beth israeliani.

[43] Sul punto vd. S. Bilgi, Intelligence Cooperation in the European Union: An Impossible Dream?, All Azimuth, v. 5, n.1, 2016, pp. 57-67.

[44] Vd. M.K.D. Cross, A European Transgovernmental Intelligence Network and the Role of IntCen, in Perspectives on European Politics and Society, vol. 14, n.3, 2013, pp. 388-402.

Altro impedimento è rappresentato dalla paura da parte degli Stati più grandi di condividere informazioni con Stati minori, più esposti al rischio di infiltrazioni. D'altro canto, gli Stati più piccoli temono che le loro agenzie possano essere inglobate da quelle degli Stati più grandi (è una delle conseguenze delle cosiddette powers asymmetries[45]). Il sentiero da seguire potrebbe essere quello di mantenere il cuore nazionale delle agenzie di intelligence europee e, allo stesso tempo, favorire tra loro un dialogo su alcuni terreni di interesse comune, come quello dell'ambiente cibernetico che, essendo per sua natura un ambiente sovranazionale, sfugge ad un controllo meramente nazionale. I benefici che deriverebbero da un sistema di condivisione di intelligence europeo strutturato possono rinvenirsi nell'ottimizzazione dei prodotti elaborati (evitando sovrapposizioni di analisi[46]), nel godere di un sostegno economico europeo a fronte dei bilanci nazionali sempre più ridotti nel settore della Difesa e nel far fronte, con maggiore efficacia, alle minacce transnazionali per la sicurezza e alla valanga globale di dati che invade il mondo dell'informazione.

Per far questo occorre, innanzitutto, diffondere una cultura europea dell'intelligence che generi fiducia[47] tra gli Stati membri e che individui una piattaforma di interessi comuni da perseguire al fine di garantire vantaggi reciproci tra le agenzie di informazione che condividono le loro attività (ad es. la lotta al terrorismo, alla criminalità informatica, alla tratta di esseri umani, alla criminalità organizzata internazionale). C'è bisogno di tempo e di un percorso graduale che mantenga distinte, nel campo della condivisione delle informazioni di intelligence, le aree di competizione da quelle di cooperazione.

La base di partenza non può che essere quella di rafforzare il quadro di cooperazione già esistente a partire, in particolare, dal ruolo dell'EU Intelligence and Situation Centre[48]. Il futuro di cooperazione dell'intelligence europea dipenderà, inoltre, da due fattori, uno interno e l'altro esterno: lo sviluppo dell'integrazione europea in materia di sicurezza e difesa e il grado di pericolo della minaccia terroristica. Sotto il profilo dell'integrazione europea, appare utile sottolineare che il 16 dicembre 2020 la Commissione europea e l'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno presentato una nuova strategia dell'UE sulla sicurezza informatica[49].

---

[45] Si veda B. Fägersten, For EU eyes only?: Intelligence and European security, in European Union Institute for Security Studies (EUISS), n.8, 2016.

[46] Su questo punto vd. A. Gruszczak, Intelligence Security in the European Union. Building a Strategic Intelligence Community, Palgrave Macmillan, Londra, 2016.

[47] Sull'importanza del tema della fiducia ai fini di creare una comunità strutturata di intelligence vd. A. Politi, Perché è necessaria un'intelligence policy europea?, in Per Aspera Ad Veritatem, n.10, 1998; J. Estevens, Building intelligence cooperation in the European Union, in Janus.net, e-journal of International Relations, Vol. 11, n. 2, 2020.

[48] In tal senso, vd. J.M. Nomikos, European Union Intelligence Analysis Centre (INTCEN): Next stop to an Agency ?, in Journal of Mediterranean and Balkan Intelligence, 22 novembre 2015.

[49] Scaricabile a questo link https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

Il documento prevede un cospicuo piano di investimenti (4,5 miliardi di euro tra il 2021 e il 2027) per rafforzare la cybersicurezza e la creazione di un'unità di coordinamento - denominata Joint Cyber Unit - tra Stati membri, UE e settore privato per la risposta agli attacchi cibernetici.

La Joint Cyber Unit è una piattaforma virtuale di cooperazione che si occuperà di coordinare la cybersecurity europea, provvedendo ad un piano di risposta alle crisi e agli incidenti cibernetici dell'UE, imperniato su piani nazionali proposti nella revisione della direttiva NIS. Si impegnerà, inoltre, a promuovere l'adozione di protocolli di mutua assistenza tra i partecipanti e a definire le capacità di monitoraggio e rilevamento nazionali e transfrontaliere. Oltre che in Europa, tuttavia, è necessario che una nuova cultura della sicurezza e dell'intelligence si affermi anche dentro i confini nazionali[50]. Sotto questo profilo, e sulla base di un'analisi comparativa, non si può sorvolare rispetto al fatto che l'Italia sia l'unico Paese del G7 a non essersi ancora dotato di una Strategia di sicurezza nazionale[51]. L'adozione di un simile strumento rappresenta un obbligo di legge per l'amministrazione degli Stati Uniti d'America fin dal 1986[52]. L'ultimo Paese del G7, in ordine cronologico, ad avere adottato la propria Strategia di sicurezza nazionale è la Germania che, il 14 giugno 2023, ha presentato la sua Nationale sicherheitsstrategie[53]. Vi è, dunque, l'urgenza di superare la frammentazione delle politiche di sicurezza nazionali, adottando una Strategia di Sicurezza Nazionale unitaria e integrata, in grado di rispondere con prontezza e lungimiranza alle sfide di un mondo in continua trasformazione.

Un passo significativo in questa direzione è stato compiuto il 24 ottobre 2024, data in cui è stata depositata la proposta di legge 2117, presentata dal deputato Lorenzo Guerini (attuale Presidente del Copasir), recante "Modifiche alla legge 3 agosto 2007, n. 124, in materia di Autorità delegata per la sicurezza della Repubblica e di strategia di sicurezza nazionale". Appare utile ricordare che con la legge 124/2007 sul «Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto», è stato riformato il comparto dell'intelligence italiana che, fino a quel momento, aveva operato sotto la vigenza della legge 801/1977[54]. La proposta di legge 2117 interviene sulla legge 3 agosto 2007, n. 124, con riguardo a tre questioni essenziali:

---

[50] Per una attualizzazione del concetto relativamente alle attuali modalità tecnologiche di compromissione del valore sicurezza, cfr. A. Pansa, La sicurezza nazionale. Innovazione e nuovi limiti, in Gnosis, 2019; G. de Vergottini, Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata, in Rivista AIC, n. 4, 2019, pp. 65-85.

[51] Sul tema si veda L. Guerini, Come cambia la sicurezza nazionale, in Formiche, Anno XX, 208, 2024, pp. 10-11; A. Soi, Ripensare l'ecosistema dell'Intelligence, in Formiche, Anno XX, 208, 2024, pp. 6-8; A. Strozzi, Sicurezza nazionale: il modello unificato che l'Italia attende e la nuova proposta di legge, in aspeniaonline.it, 8 gennaio 2025.

[52] La National Security Strategy (NSS) è un rapporto imposto dalla Sezione 603 del Goldwater-Nichols Department of Defense Reorganization Act del 1986, è stata trasmessa annualmente dal 1987.

[53] Vd. https://www.bmvg.de/de/nationale-sicherheitsstrategie.

[54] La legge 124/2007 ha subito, negli anni, diverse modifiche ed aggiornamenti, da ultimo attraverso il decreto-legge n. 48 del 2025 (c.d. decreto-legge sicurezza), che introduce rilevanti modifiche al regime delle garanzie funzionali per gli operatori dei servizi di informazione e sicurezza, ampliando sensibilmente il perimetro delle condotte autorizzate.

l'istituzione dell'Autorità delegata per la sicurezza della Repubblica, la definizione della strategia di sicurezza nazionale e l'istituzione di un Consiglio per la sicurezza nazionale. Riguardo quest'ultimo, il modello di riferimento sembrerebbe essere quello del Consiglio di sicurezza nazionale degli Stati Uniti, istituito nel 1947 dal National security act e rapidamente affermatosi come il principale interlocutore del presidente in materia di difesa e sicurezza.

Con riferimento alla figura dell'Autorità delegata, la sua nomina diverrebbe obbligatoria da parte del Presidente del Consiglio[55] e le sue funzioni potrebbero essere affidate esclusivamente a un Sottosegretario di Stato, così eliminandosi la facoltà di delegare le relative attribuzioni a un Ministro senza portafoglio.

È prevista, inoltre, l'introduzione nella legge n. 124 del 2007 del nuovo capo III-bis, dedicato alla strategia di sicurezza nazionale, adottata ogni tre anni dal Presidente del Consiglio dei ministri su proposta del Consiglio per la sicurezza nazionale.

La 'strategia di sicurezza' dovrà riguardare l'intero ambito dell'azione di governo determinando: gli interessi strategici per la sicurezza della Repubblica; gli obiettivi globali della politica estera; le minacce e i rischi cui sono esposte la collettività nazionale e le istituzioni democratiche nonché le correlate attività di prevenzione che i poteri pubblici sono chiamati a svolgere; gli indirizzi per la protezione delle infrastrutture critiche.

È da auspicare che tale proposta di legge prosegua il suo cammino e che, qualora veda la luce, la strategia di sicurezza nazionale non si riduca ad un mero adempimento burocratico ma funga da faro di orientamento per le politiche di sicurezza della Repubblica.

Il diritto alla sicurezza, infatti, non solo è da considerarsi un diritto fondamentale di natura costituzionale, ma rappresenta anche la premessa necessaria degli altri diritti costituzionali, imprescindibile per il godimento di tutte le libertà individuali[56].

---

[55] Allo stato attuale, la nomina dell'Autorità delegata è tecnicamente meramente potenziale da parte del Presidente del Consiglio dei Ministri, che non è obbligato a delegare i suoi poteri ma, come disposto dall'art.3 della l. 124/2007, può compiere tale scelta «ove lo ritenga opportuno».

[56] Sul punto, G. Cerrina Feroni, G.Morbidelli, La sicurezza: un valore superprimario, in Percorsi costituzionali, n.1/2008; T.E. Frosini, Il diritto costituzionale alla sicurezza, in forumcostituzionale.it, 2006; T.F. Giupponi, La sicurezza come valore fondamentale, in Rassegna di diritto pubblico europeo, n.2, pp. 233-259 e, dello stesso A., La sicurezza e le sue "dimensioni" costituzionali, in www.forumcostituzionale.it, 2008; C. Mosca, La sicurezza come diritto di libertà. Teoria generale delle politiche della sicurezza, Padova, 2012; M. Valentini, Sicurezza della Repubblica e democrazia costituzionale. Teoria generale e strategia di sicurezza nazionale, Editoriale Scientifica, Napoli, 2017.

FONTI PRINCIPALI

- Agenzia per la Cybersicurezza Nazionale (ACN), "Relazione annuale al Parlamento 2022", Sito istituzionale ACN, https://www.acn.gov.it/portale/relazione-annuale.
- Agenzia per la Cybersicurezza Nazionale (ACN), "Relazione annuale al Parlamento 2023", Sito istituzionale ACN, https://www.acn.gov.it/portale/relazione-annuale.
- Agenzia per la Cybersicurezza Nazionale (ACN), "CSIRT Italia — pagina dedicata (numeri 2023)", Sito istituzionale ACN, https://www.acn.gov.it/portale/csirt-italia.
- Agenzia per la Cybersicurezza Nazionale (ACN), "Rapporto sugli attacchi DoS/DDoS", 22 febbraio 2025, Sito istituzionale ACN.
- A. Alù, "Perché la disinformazione minaccia le democrazie nel 2024", AgendaDigitale.eu, 7 febbraio 2024.
- M. Artini, "Agenzia Cibernetica Nazionale italiana, confrontiamola con gli altri attori europei", AgendaDigitale.eu, 17 gennaio 2022.
- R. Baldoni, "Così l'Agenzia cyber sta lavorando e dispiega i propri effetti", AgendaDigitale.eu, 18 novembre 2021.
- R. Baldoni, Sovranità digitale. Cos'è e quali sono le principali minacce al cyberspazio nazionale, Bologna, Il Mulino, 2025.
- R. Baldoni, "Il ruolo guida dell'Agenzia per la Cybersicurezza Nazionale (ACN) verso la Cyber-Resilienza Nazionale: sinergie pubblico-private", in U. Gori (a cura di), Cyber Warfare 2021-2022. Cibersicurezza: dalla collaborazione Pubblico-Privato alla difesa dello Stato, Milano, Franco Angeli, 2023, 21-25.
- S. Bilgi, "Intelligence Cooperation in the European Union: An Impossible Dream?", All Azimuth, 5(1), 2016, 57-67.
- F. Bechis, "Non solo cyber, così riformiamo l'intelligence. Parla Franco Gabrielli", Formiche.net, 14 agosto 2021.

- G. Carrer, “Riforma dell’intelligence? Sì, dicono Pagani (Pd), Perego (FI) e Tofalo (M5S)”, Formiche.net, 29 luglio 2021.
- M. Caligiuri, Come i pesci nell’acqua. Immersi nella disinformazione, Soveria Mannelli, Rubbettino, 2019.
- M. Caligiuri, A. Pagani, M. Chioso, Disinformare: ecco l’arma. L’emergenza educativa e democratica del nostro tempo, Soveria Mannelli, Rubbettino, 2024.
- M. Caligiuri, Cyber intelligence. Tra libertà e sicurezza, Roma, Donzelli, 2016.
- M. K. D. Cross, “A European Transgovernmental Intelligence Network and the Role of IntCen”, Perspectives on European Politics and Society, 14(3), 2013, 388-402.
- B. Fägersten, For EU Eyes Only? Intelligence and European Security, EUISS Brief, n. 8, 2016.
- I. Galimova, “L‘operazione militare speciale’ in Ucraina e la reazione del sistema politico russo”, Nomos. Le attualità del diritto, 1, 2022.
- GCHQ — Government Communications Headquarters, “Our Origins and WWI”, Sito ufficiale, Cheltenham, https://www.gchq.gov.uk/.
- L. Guerini, “Come cambia la sicurezza nazionale”, Formiche, Anno XX, n. 208, 2024, 10-11.
- A. Gruszczak, Intelligence Security in the European Union. Building a Strategic Intelligence Community, London, Palgrave Macmillan, 2016.
- H. Kissinger, Ordine mondiale, Milano, Mondadori, 2017, 339.
- M. C. Libicki, “The Convergence of Information Warfare”, Strategic Studies Quarterly, 11(1), 2017, 49-65.
- M. L. Mariscal, International Cybersecurity: Law, Policy, and Strategy, Oxford, 2020.
- A. Monti, “Il rinnovamento dell’intelligence ha bisogno di coerenza normativa”, Formiche.net, 6 dicembre 2020.

- F. Nisticò, “L’elemento cyber nella guerra russo-ucraina”, Aspeniaonline.it, 3 marzo 2022.
- J. M. Nomikos, “European Union Intelligence Analysis Centre (INTCEN): Next Stop to an Agency?”, Journal of Mediterranean and Balkan Intelligence, 22 novembre 2015.
- A. Pagani, “La guerra cibernetica nell’età ibrida: tecnologie, strategie e priorità”, AgendaDigitale.eu, 22 luglio 2021.
- F. Pizzetti, “La protezione dei dati personali nell’era digitale: sfide e prospettive”, in G. Scorza, A. Sica (a cura di), Cybersecurity e privacy: nuove frontiere del diritto, Roma, 2022, 89-112.
- O. Pollicino, G. Pitruzzella, Disinformation and Hate Speech. A European Constitutional Perspective, Milano, Egea, 2020.
- C. Pinelli, C. Hassan, Disinformazione e democrazia, Venezia, Marsilio, 2022.
- Presidenza del Consiglio dei Ministri — Dipartimento delle Informazioni per la Sicurezza (DIS), Relazione sulla politica dell’informazione per la sicurezza 2023, Roma.
- M. Santarelli, “Relazione Intelligence 2023: la risposta dell’Italia a minacce ibride e conflitti globali”, AgendaDigitale.eu, 7 marzo 2024.
- U. Saccone, “Quale intelligence per il futuro?”, Formiche.net, 2 agosto 2021.
- M. Sbailò, “Guerre ibride: quali risposte possibili?”, DPCE online, 63(SP1), 2024.
- A. Soi, “Ripensare l’ecosistema dell’Intelligence”, Formiche, Anno XX, n. 208, 2024, 6-8.
- A. Spaziani, “L’attacco cibernetico nell’era della guerra ibrida”, DPCE online, 63(SP1), 2024.
- M. Vedaschi, À la guerre comme à la guerre. La disciplina della guerra nel diritto costituzionale comparato, Torino, 2007.
- G. de Vergottini, Guerra e costituzione. Nuovi conflitti e sfide alla democrazia, Bologna, Il Mulino, 2004.