AIC Associazione Italiana dei Costituzionalisti

Rivista AIC

Trimestrale di diritto costituzionale

Anno 2025/ Fascicolo IV • Supplemento

Contributi di R. Balduzzi, L. Chieffi, M. Cavino, A. Vedaschi, A. Bultrini, V. Ciaccio, B. Pezzini, C. De Fiores, B. Nascimbene, D. Cabras, P. Bonetti, L. Buffoni, R. Ibrido, M. Malvicini, C. Pannacciulli, M. Plutino

L'Associazione Italiana dei Costituzionalisti è iscritta al Registro degli Operatori della Comunicazione a far data dal 09.10.2013 con n. 23897.

Codice ISSN 2039-8298 (Online). La Rivista dell'Associazione Italiana dei Costituzionalisti è inoltre registrata presso il Tribunale di Roma - n.339 del 05.08.2010.

Rivista trimestrale inclusa nella classe A delle Riviste scientifiche dell'Area 12 - Scienze giuridiche

RIVISTA AIC ASSOCIAZIONE ITALIANA DEI COSTITUZIONALISTI

Supplemento al fascicolo n° 4/2025
Data di pubblicazione: 13/03/2026

Autore: Massimiliano Malvicini*

Il "quinto dominio" e l'ordinamento costituzionale: contributo allo studio della ripartizione delle competenze in materia di *sicurezza nazionale cibernetica* in Italia

1. L'uso della forza e il ciberspazio.

All'interno della riflessione sul tema dell'uso della forza e, allo stesso tempo, sul rapporto fra il concetto di pace e quello di guerra nel nostro ordinamento costituzionale può essere utile soffermarsi su una nozione che ha assunto una crescente centralità all'interno del dibattito contemporaneo: quella di ciberguerra (*cyberwarfare*)[1].

La rilevanza di questo termine nell'ambito delle relazioni internazionali e della riflessione scientifica – giuridica e non – scaturisce, almeno in parte, dal suo riferirsi ad un fenomeno ibrido[2],

* Ricercatore di Diritto costituzionale e pubblico – Università degli Studi del Piemonte Orientale "Amedeo Avogadro".

[1] Su cui v., S. PIETROPAOLI, *Un altro modo di fare la guerra. La cyberwar come problema giuridico*, in *Ars interpretandi*, 2023, I, 61 ss.

[2] Sul concetto di "guerra ibrida" v. la recente ricostruzione di A. SPAZIANI, *L'attacco cibernetico nell'era della guerra ibrida*, in *DPCE online*, 2024, I, 511 ss., nonché, nell'ambito di *questo fascicolo*, L. CHIEFFI, *Pace e guerra in un'epoca di profonde trasformazioni delle relazioni internazionali;* P. BONETTI, *Il dovere costituzionale di difendere la patria di fronte alle nuove minacce*; M. PLUTINO, *La crisi di prescrittività della "costituzione della difesa". Continuum e sovrapposizione pace/guerra nel nuovo contesto tecnologico e delle relazioni internazionali*.

L'Associazione Italiana Costituzionalisti è iscritta al Registro Operatori della Comunicazione dal 9.10.2013, n. 23897
La Rivista AIC è inclusa nella classe A delle Riviste scientifiche dell'Area 12 - Scienze giuridiche | ISSN 2039-8298 (on-line)
Direttore responsabile: prof. Renato Balduzzi
Direttori: prof. Andrea Pertici (coord.), prof.ssa Benedetta Liberali, prof.ssa Lucia Scaffardi, prof.ssa Giusi Sorrenti

capace di mettere in discussione i paradigmi geopolitici e normativi consolidatisi nel corso dei decenni, a partire dalla loro capacità interpretativa e dall'attitudine prescrittiva. A essere significative, in questa qualificazione, sono alcune sue caratteristiche, che a loro volta sono espressione del particolare dominio in cui essa prende le mosse: il ciberspazio. Si pensi, a tale riguardo, alla sistematica difficoltà nell'identificare con certezza l'origine statuale o non-statuale di un'azione ostile, da cui derivano le difficoltà a reagire secondo gli strumenti del diritto convenzionale; alla deterritorializzazione del conflitto, resa possibile dalla natura transnazionale delle reti digitali, la quale non solo relativizza il concetto di fronte geograficamente definito ma contribuisce a trasformare l'infrastruttura Internet in un potenziale teatro operativo *sine die*; alla capacità di far convergere strumenti e metodi di offesa eterogenei (militari e tecnologici, ma anche informativi, economici e diplomatici, in modo del tutto asimmetrico) spaziando dallo spionaggio al sabotaggio di infrastrutture critiche, militari e civili, passando per la propaganda e la disinformazione (cd. *information warfare*).

Come noto, tra le numerose sfide che la ciberguerra pone agli studiosi, quella relativa al suo inquadramento nelle categorie del diritto positivo – a partire da quello internazionale (cui del resto la nostra Costituzione fa rinvio) – è di grande interesse.

In tale direzione, è utile ricordare che, ad esempio, sottolineando come l'uso della forza che si manifesta nell'ambito del ciberspazio si dispieghi su tre livelli – quello *fisico,* costituito da tutte le infrastrutture *hardware* che contengono, trasportano ed elaborano i dati; quello *logico*, dato dal codice, dalle istruzioni e dai dati che governano il funzionamento delle infrastrutture fisiche; quello *sociale*, che consiste nell'interazione tra le persone fisiche che accedono alla rete e nel modo in cui interagiscono con le informazioni e la percezione che hanno della realtà mediata dalla tecnologia, così come nelle interazioni fra macchine[3] – la dottrina abbia argomentato in favore dell'applicabilità dei principi di diritto internazionale alle ciber-minacce in virtù del principio di equivalenza degli effetti (*effect-based approach*): se un'operazione cibernetica produce effetti equivalenti a quelli di un'azione fisica/cinetica, allora dev'essere soggetta alle medesime norme giuridiche.

Nel complesso, il consolidamento di questa impostazione è il prodotto di due processi paralleli e complementari – uno di natura politica, sostenuto dal lavoro del Gruppo di Esperti Governativi delle Nazioni Unite (UN GGE), la cui funzione è stata cruciale nel contrastare le tesi "ciber-eccezionaliste"; l'altro di natura dottrinale, che ha trovato la sua codificazione più autorevole nel *Tallinn Manual*, opera elaborata dal *NATO Cooperative Cyber Defence Centre of Excellence* a seguito delle vicende della *Web War One* nel 2013 e aggiornato nel 2017[4] – ai quali, oggi più che mai, è

[3] Si accoglie, in questa sede, la tripartizione suggerita da D.T. KUEHL, *From Cyberspace to Cyberpower: Defining the Problem*, in F.D. KRAMER – S.H. STARR – L. K. WENTZ (eds.), *Cyberpower and National Security,* University of Nebraska Press, Lincoln, 2009, 24 ss. e accolta anche da L. MARTINO, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica e società*, 2018, I, 64 ss.

[4] Il quale stabilisce, per l'appunto, che un'operazione cibernetica costituisce un "uso della forza" quando la sua scala e i suoi effetti sono comparabili a quelli di operazioni non cibernetiche che raggiungono tale soglia (regola n. 11) mentre definisce l'"attacco cibernetico" come un'operazione ragionevolmente suscettibile di causare lesioni, morte, o

opportuno far riferimento, anche considerando come essi forniscano interessanti spunti ermeneutici utili per facilitare l'applicazione dei principi di diritto internazionale alle minacce cibernetiche, a partire da quelli in materia di attribuzione della condotta informatica illecita perpetrata da soggetti privati ad uno Stato, di cui al Progetto di Articoli sulla Responsabilità degli Stati per Atto Internazionalmente Illecito del 2001, e quelli in materia di obblighi di monitoraggio e prevenzione di operazioni ostili nei confronti degli altri Stati (cd. *due diligence*), di cui la sentenza della Corte internazionale di giustizia nel caso Canale di Corfù (1949)[5].

2. Poteri e competenze nell'ordinamento italiano di fronte alle ciber-minacce.

Come noto, l'emergere della ciberguerra ha provocato una serie di conseguenze non solo nell'ambito del diritto internazionale, ma anche all'interno dei singoli ordinamenti statali. Tra le principali conseguenze va identificato l'abbandono – nei processi di elaborazione delle politiche pubbliche in materia di sicurezza – del tradizionale paradigma volto alla salvaguardia dei confini "fisici" in favore dell'adozione di quello "securitario" (nelle sue molteplici declinazioni)[6]: circostanza che, nel contesto italiano, ha portato all'emersione di una specifica macro-funzione dai contenuti incerti[7] e, correlativamente, di un ampio complesso istituzionale di cui componente essenziale è, non a caso, l'architettura nazionale in materia di sicurezza cibernetica[8].

In termini generali, l'attuale assetto istituzionale in materia di difesa contro i ciberattacchi è il risultato di un processo sviluppatosi dal 2012[9]: a quel tempo, le minacce provenienti dal "quinto dominio" furono declinate soprattutto come un problema di sicurezza dello Stato e di *intelligence*. Vennero quindi aumentate le competenze del Sistema di Informazione per la Sicurezza della

---

il danneggiamento e la distruzione di oggetti fisici (regola n. 92). Cfr. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, general editor M.N. Schmitt, Cambridge, 2017.

[5] Su questi aspetti cfr. A. BONFANTI, *Attacchi cibernetici in tempi di pace: le intrusioni nelle elezioni presidenziali statunitensi del 2016 alla luce del diritto internazionale*, in *Rivista di diritto internazionale*, 2019, III, 710 ss.; G. DELLA MORTE, *Limiti e prospettive del diritto internazionale del cyberspazio*, in *Rivista di diritto internazionale*, 2022, I, 12 ss.

[6] Su questa dinamica v. R. URSI, *Editoriale – La difesa: tradizione e innovazione*, in *Diritto costituzionale*, 2022, I, a cura di R. Ursi, 10 ss.

[7] Su cui cfr. T.F. GIUPPONI, *I rapporti tra sicurezza e difesa. Differenze e profili di convergenza*, in *Diritto costituzionale*, 2022, I, a cura di R. Ursi, 34; R. URSI, *La sicurezza cibernetica come funzione pubblica,* in R. URSI (a cura di), *La sicurezza nel cyberspazio*, FrancoAngeli, Milano, 2023, 7 ss.; G. DE VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata,* in *Rivista AIC*, 2019, 4. Sotto una diversa prospettiva v. E. PIZZIMENTI – A. VANNUCCI, *Il concetto di sicurezza e le politiche per la sicurezza*, in *Rivista trimestrale di scienza dell'amministrazione*, 2005, IV, 51 ss.

[8] Per un primo inquadramento del concetto di cybersecurity si v. D. SCHATZ – R. BASHROUSH – J. WALL, *Towards a More Representative Definition of Cyber Security*, in *Journal of Digital Forensics, Security and Law*, 2017, II, 53-74.

[9] Per una ricostruzione in termini analitici di questo processo v. T.F. GIUPPONI, *Il governo nazionale della cybersicurezza*, in *Quaderni costituzionali*, 2024, 2, 277-302. Per un'analisi dei principali profili che riguardano l'attuale assetto della sicurezza nazionale cibernetica si vedano i due fascicoli di *Teoria e critica della regolazione sociale*, dal titolo *Cybersecurity e istituzioni democratiche. Un'indagine interdisciplinare: diritto, informatica e organizzazione aziendale*, 2024, II (a cura di G. Bombelli e S. Rossa) e 2025, I (a cura di P. Heritier e S. Rossa).

Repubblica, così come riformato dalla legge 124 del 2007[10]: questo passaggio si perfezionò mediante l'approvazione della legge 7 agosto 2012, n. 133[11] e, soprattutto, con l'emanazione del DPCM 24 gennaio 2013, recante la direttiva sugli "indirizzi per la protezione cibernetica e la sicurezza informatica nazionale" (cd. "direttiva Monti").

Nello specifico, il DPCM 24 gennaio 2013 individuò nella Presidenza del Consiglio dei Ministri il vertice dell'architettura nazionale in materia di sicurezza cibernetica, tanto che a esso fu affidato il potere di adottare: a) il quadro strategico nazionale per la sicurezza dello spazio cibernetico, entro il quale andavano indicati profili e tendenze evolutive delle minacce e delle vulnerabilità dei sistemi e delle reti di interesse nazionale, ma anche la definizione dei ruoli e dei compiti dei vari soggetti, pubblici e privati; b) su deliberazione del Comitato Interministeriale Sicurezza della Repubblica (CISR), il Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali, contenente obiettivi da conseguire e linee di azione da porre in essere per realizzare il quadro strategico nazionale; c) il potere di impartire, sentito il CISR, le direttive al Dipartimento delle Informazioni per la Sicurezza (DIS), all'Agenzia informazioni e sicurezza interna (AISI) e all'Agenzia informazioni e sicurezza esterna (AISE).

In quell'assetto, un ruolo di primo piano fu riconosciuto al Nucleo per la sicurezza cibernetica (NSC), organo istituito presso il Consigliere militare del presidente del Consiglio (cui spettava la presidenza). Esso era composto, fra gli altri, dai rappresentanti del DIS, dell'AISE, dell'AISI, del Ministero degli Affari esteri, del Ministero dell'Interno, del Ministero della Difesa e del Ministero dello Sviluppo economico. All'NSC furono affidate funzioni di grande rilevanza in materia di prevenzione e preparazione a situazioni di crisi, attivazione delle procedure di allertamento e coordinamento inter-istituzionale (ad esso spettava il compito di raccordare le varie componenti coinvolte nella salvaguardia della sicurezza cibernetica, ma anche quello di pianificare le risposte a scenari di crisi cibernetica).

Successivo a tali provvedimenti è il principale documento di *policy* che si può considerare il punto di partenza per l'elaborazione di una strategia in materia di difesa cibernetica sotto il versante militare. Ci si riferisce, nello specifico, al "Libro Bianco per la Sicurezza Internazionale e la Difesa", presentato dal Ministro Pinotti al Consiglio Supremo di Difesa e alle commissioni riunite III e IV della Camera e del Senato nel maggio 2015: in esso trovarono spazio i richiami alla necessità di sviluppare, accanto alle capacità più tradizionali, «le possibilità di difesa contro attacchi di natura cibernetica che dovessero eccedere le capacità predisposte dalle agenzie civili» (punto 68) dedicando a esse specifiche capacità operative difensive, tutto ciò al fine di preservare la sicurezza del "sistema Paese" e di rafforzare la tenuta delle strutture politiche, economiche e sociali (punto 103); tale obiettivo avrebbe dovuto orientare sia la razionalizzazione delle strutture

[10] Sulla riforma del 2007 v. T.F. GIUPPONI, *Servizi di informazione e segreto di Stato nella legge n. 124/2007*, in A. CARIOLA – E. CASTORINA – A. CIANCIO (a cura di), *Studi in onore di Luigi Arcidiacono*, vol. IV, Giappichelli, Torino, 2010, 1677-1751; C. MOSCA – S. GAMBACURTA – G. SCANDONE – M. VALENTINI, *I servizi di informazione e il segreto di stato (Legge 3 agosto 2007, n. 124)*, Giuffrè, Milano, 2008; G. ILLUMINATI (a cura di), *Nuovi profili del segreto di Stato e dell'attività di intelligence*, Giappichelli, Torino, 2010.

[11] Su cui cfr. G. SCACCIA, *Intelligence e segreto di Stato nella legge n. 133 del 2012*, in *Diritto e società*, 2012, III, 585-599.

direttive e di comando del comparto della difesa, riconoscendo un ruolo di primo piano al Comando Interforze per le Operazioni Cibernetiche presso il Comando Operativo di Vertice Interforze (punto 173), sia i processi di integrazione delle capacità italiane nel complesso delle forze NATO, al fine di contrastare eventuali aggressioni militari che si dovessero manifestare contro l'Italia e i suoi interessi vitali, operando nelle cinque dimensioni, tra le quali quella cibernetica (punto 195).

Come noto, nonostante questi intendimenti, negli anni successivi fu soprattutto il sistema sotto la responsabilità diretta del presidente del Consiglio dei Ministri a mantenere la centralità sulle politiche in materia di sicurezza nazionale cibernetica, pur confermando l'impostazione originaria fondata sulla centralità del comparto intelligence.

Così, attraverso l'approvazione del DPCM 17 febbraio 2017 (recante la "Direttiva in materia protezione cibernetica e sicurezza informatica nazionali", il cd. "Decreto Gentiloni"), vennero attribuite al presidente del Consiglio specifiche competenze per far fronte agli scenari di crisi nazionale. Parallelamente, furono potenziate le attribuzioni del DIS, affidando al suo direttore generale il compito di definire le necessarie linee di azione per innalzare i livelli di sicurezza di reti e sistemi, e incardinando al suo interno il Nucleo per la Sicurezza Cibernetica (presieduto da un vicedirettore generale del Dipartimento, su delega del direttore generale).

A un anno di distanza, in attuazione della direttiva UE 2016/1148 (c.d. direttiva NIS – *Network and Information Security*) – il cui obiettivo era stabilire misure per uno standard comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione al fine di aumentare il livello di collaborazione nella prevenzione delle minacce cibernetiche[12] – intervenne il decreto legislativo 18 maggio 2018, n. 65. Quest'ultimo, fra l'altro, attribuì al presidente del Consiglio la competenza alla definizione della strategia nazionale di sicurezza cibernetica per la tutela delle reti e dei sistemi di interesse nazionale (sentito il CISR). Al D.Lgs. 65/2018 è poi seguito il decreto-legge 21 settembre 2019, n. 105 (il c.d. "decreto perimetro")[13] con cui non solo si accrebbero ulteriormente le competenze del presidente del Consiglio, conferendo a esso uno specifico potere di ordinanza in materia, ma – soprattutto – fu superato il precedente paradigma securitario basato sulla cooperazione volontaria dei soggetti privati coinvolti nell'esercizio di funzioni essenziali per lo Stato.

Negli stessi anni, il settore militare visse una stagione di consolidamento cercando di implementare le indicazioni del Libro bianco del 2015.

A livello esterno, una spinta in tal senso giunse dal Summit di Varsavia del 2016, che produsse una dichiarazione (la *Cyber defence pledge*) ove i Capi di Stato e di Governo dei Paesi NATO

---

[12] Sulle iniziative europee e il loro intreccio con l'ordinamento italiano cfr. A. CONTALDO – L. SALANDRI, *La disciplina della cybersecurity nell'Unione Europea*, in A. CONTALDO – D. MULA (a cura di), *Cybersecurity law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pacini Giuridica, Pisa, 2020, 1-55; E.C. RAFFIOTTA, *Cybersecurity regulation in the European Union and the issues of Constitutional law*, in questa *Rivista*, 2022, IV; L. MORONI, *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, in *Federalismi.it*, 2024, XIV, 185 ss.

[13] Su cui v. L. CALANDRIELLO, *Il perimetro di sicurezza nazionale cibernetica,* in *La sicurezza nel cyberspazio*, 139-151; S. POLETTI, *La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro nazionale di sicurezza cibernetica*, in *Media-Laws,* 2023, II, 398 ss.

riaffermarono la centralità del ciberspazio (definito come "dominio operazionale"). Nel contempo, essi sancirono la volontà di potenziare gli strumenti di ciberdifesa dell'Alleanza (tale documento fu ripreso anche nei vertici successivi, come quello di Bruxelles, e rappresenta uno dei presupposti su cui si è articolato l'attuale quadro strategico atlantico).

A livello interno, particolarmente rappresentativi degli sforzi compiuti in questa fase furono il Piano Nazionale per la protezione Cibernetica e la Sicurezza Informatica del 2017, i Documenti Programmatici Pluriennali (DPP) e, infine, le dichiarazioni programmatiche dei ministri della Difesa Trenta (2018-2019) e Guerini (2019-2021). Quanto al Piano Nazionale, il «Potenziamento delle capacità di intelligence, di polizia e di difesa civile e militare» fu oggetto del primo indirizzo operativo: a tal fine, vennero indicati come prioritari l'istituzione di «strutture preposte alla difesa dello spazio cibernetico» (1.4, lett. "a") e lo sviluppo di «strutture di Comando e Controllo in grado di pianificare e condurre operazioni militari nello spazio cibernetico in maniera efficace» (1.4 lett. "b").

Come accennato, anche Documenti Programmatici Triennali, a partire da quello del 2017-2019, iniziano a delineare la necessità di una «capacità interforze di Cyber Defence», mediante programmi di investimento volti ad assicurare la «protezione, la resilienza e la capacità di risposta» delle reti della Difesa; un obiettivo, questo, rimarcato in tutti i documenti successivi con crescente intensità (2018-2020, 2019-2021; 2020-2022). A suggellare politicamente le traiettorie definite da tali documenti furono poi le dichiarazioni dei ministri succedutisi a Palazzo Baracchini. Esse testimoniano una piena consapevolezza circa la necessità di superare la frammentazione del quadro operativo allora vigente[14] e di dotare il Paese di «una capacità cibernetica completa, che includa anche una dimensione offensiva credibile, quale strumento di deterrenza e risposta»[15].

Sul piano istituzionale, queste linee di indirizzo portarono a una prima razionalizzazione nel coordinamento delle competenze in materia di ciberdifesa distribuite presso le singole Forze Armate (Esercito, Marina, Aeronautica) prevedendo un unico polo interforze, ossia il Comando Interforze per le Operazioni Cibernetiche (CIOC), istituto nel settembre 2017 e poi incorporato, anche a seguito dell'emanazione del Concetto strategico del Capo di Stato Maggiore della Difesa del gennaio 2020, in una nuova struttura presso lo Stato maggiore della Difesa: il Comando per le Operazioni in Rete (COR)[16]. Posto sotto la responsabilità del Capo di Stato Maggiore della Difesa, come suggerito dal Libro Bianco del 2015, il COR fu articolato in tre reparti: il Reparto C4, il Reparto Sicurezza e *Cyber Defence* e il Reparto *Cyber Operations* (nel quale confluì il CIOC), cui fu conferita la competenza di esercitare le attività militari cibernetiche, volte alla salvaguardia dei sistemi e dei servizi della Difesa, in relazione non solo al territorio nazionale, ma anche ai vari teatri operativi. A tal fine, all'interno del reparto operano le Cellule Operative Cibernetiche

---

[14] V. Atti Parlamentari, Senato della Repubblica, XVII legislatura, Audizione del Ministro della Difesa, Elisabetta Trenta, sulle linee programmatiche del suo dicastero, 26 luglio 2018.

[15] V. Atti parlamentari, Camera dei deputati, XVII legislatura, Audizione del Ministro della Difesa, Lorenzo Guerini, sulle linee programmatiche del suo dicastero, 28 novembre 2019.

[16] A. MARRONE – O. CREDI, *Il Comando per le Operazioni in Rete (COR),* in A. MARRONE – E. SABATINO – O. CREDI (a cura di), *L'Italia e la difesa cibernetica*, Istituto Affari Internazionali - Documenti IAI, settembre 2021, 11 ss.

(COC): team di specialisti interforze in grado di condurre operazioni difensive e offensive, anche in scenari di crisi, al fine di ridurre il livello di vulnerabilità cui sono soggette sia le infrastrutture cibernetiche sul territorio italiano sia i contingenti dispiegati all'estero nell'ambito delle missioni internazionali.

Ad ogni buon conto, si dovette aspettare il 2021 per assistere a una riforma dell'assetto istituzionale in materia di sicurezza nazionale che riuscisse a creare i presupposti per un coordinamento fra il comparto della Presidenza del Consiglio e quello del Ministero della Difesa anche in materia cibernetica.

All'interno del disegno razionalizzatore recato dal decreto-legge 14 giugno 2021, n. 82 (convertito con modificazioni dalla l. 4 agosto 2021, n. 109)[17] – dei cui profili non si può dar conto in questa sede – furono infatti previste due specifiche sedi di raccordo.

La prima, di tipo politico, fu identificata nel Comitato Interministeriale per la Cybersicurezza (CIC). A questo è conferito il compito di proporre al presidente del Consiglio dei ministri gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza nazionale. Esso esercita l'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza e promuove l'adozione delle iniziative necessarie per favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza. Il CIC è presieduto dal presidente del Consiglio (al quale, è bene rammentarlo, è conferita l'alta direzione e la responsabilità generale delle politiche di cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico; l'adozione della strategia nazionale di cybersicurezza, sentito il CIC, la nomina e la revoca dei vertici dell'Agenzia per la cybersicurezza nazionale) e a esso partecipano i vertici di altri dicasteri ritenuti "strategici", tra i quali vi è per l'appunto il Ministro della Difesa (art. 4, c. 3).

La seconda, di tipo operativo, è costituita dall'Agenzia per la cybersicurezza nazionale (ACN)[18]. Essa ha il compito di promuovere una maggiore tutela e resilienza rispetto alle minacce cibernetiche (sviluppando le capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta). Ciò ha lo scopo di prevenire e gestire attacchi informatici nonché incidenti di sicurezza informatica. A tal fine, presso l'Agenzia opera il Nucleo per la Cybersicurezza (NCS), la cui composizione riprende, pur con qualche variazione, quella dell'originario Nucleo per la Sicurezza Cibernetica (istituito nel 2013 e transitato, nel 2017, sotto l'egida del DIS): accanto al Consigliere militare del presidente del Consiglio dei ministri e ai rappresentanti del comparto intelligence (i.e. DIS, AISE e AISI), a esso partecipano i rappresentanti delle altre componenti del sistema, tra cui proprio il Ministero della Difesa.

---

[17] Su cui cfr. F. SERINI, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in *Federalismi.it*, 2022, XII, 241-272.

[18] Su cui cfr. L. PARONA, *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, in *Giornale di diritto amministrativo*, 2021, VI, 709 ss.; I. FORGIONE, *Il ruolo strategico dell'agenzia nazionale per la cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna*, in *Diritto amministrativo*, 2022, IV, 1113 (anche in *La sicurezza nel cyberspazio*, cit., 95-121); S. ROSSA, *Cybersicurezza e Pubblica Amministrazione*, Editoriale Scientifica, Napoli, 2023, 91 ss.

3. Riflessioni conclusive.

A differenza di un decennio fa, si può affermare che ad oggi il comparto facente capo al presidente del Consiglio dei Ministri e quello di cui è responsabile il Ministro della Difesa convergono verso la realizzazione di una politica integrata di sicurezza nazionale. Tale processo è legittimato, ora, non solo sul piano amministrativo – si pensi all'impiego di personale del Ministero della Difesa presso l'Agenzia, perfezionatosi mediante l'emanazione del DPCM 24 luglio 2024[19]; passaggio a cui sono seguite, più di recente, ulteriori forme di collaborazione, come attesta la firma dell'Atto d'Intesa tra lo Stato Maggiore della Difesa e l'ACN del giugno 2025 – ma anche sul piano normativo, considerato come, alla luce della novella recata dall'art. 51, c. 8, lett. "e" del d.l. 17 maggio 2022, n. 50, convertito con modificazioni dalla legge 15 giugno 2022, n. 91, l'art. 88 del Codice dell'ordinamento militare sancisce come lo strumento militare sia volto a «consentire la permanente disponibilità di strutture di comando e controllo di Forza armata e interforze, facilmente integrabili in complessi multinazionali, e di *unità* terrestri, navali, aeree, *cibernetiche* e aero-spaziali di intervento rapido, preposte alla difesa del territorio nazionale, delle vie di comunicazione marittime e aeree, *delle infrastrutture* spaziali e *dello spazio cibernetico in ambito militare*; è finalizzato, altresì, alla partecipazione a missioni anche multinazionali per interventi a supporto della pace»[20].

Naturalmente, come è stato opportunamente evidenziato dalla dottrina, oltre che dagli operatori del settore, dinanzi all'attuale quadro la questione del coordinamento fra queste due "anime" dell'architettura di sicurezza nazionale è tutt'altro che risolta. In particolare, per i profili che interessano in questa sede[21], a dover essere centrale per gli studiosi è soprattutto il tema dei poteri (e, dunque, delle correlative responsabilità) che spettano, rispettivamente, al presidente del Consiglio e al Ministro della Difesa; ciò, anche in virtù della possibilità che, nell'ambito del "quinto dominio", si verifichino casi in cui, di fronte a minacce per la sicurezza nazionale, non siano sufficienti azioni di mera resilienza, ma siano necessarie azioni offensive, circostanza che – di là dalle formule di rito previste dall'art. 7-ter, c. 3 del d.l. 174/2015[22] – avvicina le decisioni in materia di sicurezza nazionale all'alveo dei principi previsti dal nostro ordinamento in materia

[19] Ex art. 12, c. 1 del d.l. 82/2021, con cui è stato disposto l'incardinamento, all'interno dell'Agenzia, di un plesso dotato di un suo peculiare status – la cd. "Struttura Difesa" – data la contemporanea subordinazione dei suoi membri ad una dipendenza di tipo gerarchico nei confronti Capo di Stato maggiore della Difesa e ad un'altra di tipo funzionale rispetto al direttore generale dell'ACN.

[20] V. altresì Strategia Nazionale di Cybersicurezza 2024-2026 – Piano di implementazione, 29 ss.

[21] Sulle problematiche legate al rapporto tra il settore "intelligence" e la stessa ACN v. M. MACCHIA – G. SFERRAZZO, *Sicurezza e rischio tecnologico. La funzione di cybersecurity,* in *Diritto amministrativo*, 2025, I, 115 ss.

[22] Come novellato dal d.l. 9 agosto 2022, n. 115 convertito con l. 21 settembre 2022, n. 142.

bellica[23], rilanciando gli interrogativi sulla necessità di predisporre un ulteriore perfezionamento della governance del comparto coinvolgendo le competenze di altri organi, a partire per esempio dal Consiglio Supremo di Difesa[24], senza tralasciare quelli di matrice parlamentare, come testimonia il dibattito scientifico sviluppatosi a seguito della cessione di armi ed equipaggiamenti bellici alla Repubblica Ucraina nel 2022[25].

Titolo [En]: The "Fifth Domain" and the Constitutional Order: A Contribution to the Study of the Distribution of Powers in Matters of National Cybersecurity in Italy.

Abstract [It]: Il saggio analizza le sfide che il ciberspazio, quale "quinto dominio" del confronto strategico, pone all'ordinamento costituzionale italiano, con particolare riferimento alla ripartizione delle competenze in materia di sicurezza nazionale. La prima parte del contributo ricostruisce l'inquadramento della minaccia cibernetica nel diritto internazionale. La seconda parte, cuore dell'analisi, ripercorre l'evoluzione dell'architettura istituzionale italiana, mostrando la progressiva emersione di un doppio binario di competenze: uno facente capo alla Presidenza del Consiglio dei Ministri, e uno sotto la responsabilità del Ministero della Difesa. Nelle conclusioni, pur riconoscendo i recenti sforzi di razionalizzazione, si evidenzia come la questione del coordinamento dei poteri, specie in relazione a possibili azioni offensive, rimanga aperta, suggerendo la necessità di un'ulteriore riflessione in materia.

Abstract [En]: This essay analyzes the challenges that cyberspace, as the "fifth domain" of strategic confrontation, poses to the Italian legal system, with particular reference to the distribution of powers in national security matters. The first part of the contribution reconstructs the framing of cyber threats in international law. The second part, traces the evolution of the Italian institutional architecture, showing the gradual emergence of a dual track of competencies: one headed by the Presidency of the Council of Ministers, and one under the responsibility of the Ministry of Defence. In conclusion, while acknowledging recent rationalization efforts, the essay points out that the issue of coordinating powers, especially concerning potential offensive actions, remains unresolved, suggesting the need for further reflection.

Parole chiave [It]: Cibersicurezza; Ciberguerra; Uso della forza; Sicurezza nazionale; Ordinamento costituzionale italiano.

Keywords [En]: Cybersecurity; Cyberwarfare; Use of Force; National Security; Italian Legal System.

---

[23] Su cui v. M. CAVINO, *L'esperienza della guerra in epoca repubblicana*, in *questo fascicolo*; ID., *Il governo della guerra*, in *Quaderni costituzionali*, 2022, IV, 753-778; nonché, volendo, M. CAVINO – M. MALVICINI, *Le guerre dell'Italia repubblicana,* Bologna, il Mulino, 2023, 129 ss.

[24] Sul punto v. i rilievi di T.F. GIUPPONI, *I rapporti tra sicurezza e difesa*, cit., 46-47.

[25] Su cui v. P. GAMBALE – G. PICCIRILLI, *Il controllo parlamentare su missioni all'estero e cessione di armamenti. Spunti ricostruttivi e profili evolutivi nelle legislature XVIII e XIX*, in P. GAMBALE – N. LUPO – A. SANDULLI – M. SEROWANIEC (a cura di), *Sicurezza e Democrazia. Atti del X Colloquio italo-polacco sulle trasformazioni istituzionali*, Bari-Foggia 19-20 ottobre 2023, Giappichelli, Torino, 2025, 439 ss.