PIER GIORGIO CHIARA

Il governo della cybersicurezza: crisi dello Stato? Potere, diritto e vulnerabilità nell'era digitale globale[*]

Abstract. Cybersecurity poses significant challenges for legal theory, unsettling fundamental categories such as sovereignty, responsibility, and normativity. The modern paradigm of security, based on the idea that the State is the exclusive guarantor of public order within territorially defined boundaries, falters when confronted with cyber threats that unfold in an extraterritorial, transnational, technically opaque and (mostly) privately owned and managed domain, that is, cyberspace. In the EU, cybersecurity governance operates through a multi-level and multi-stakeholder architecture in which public and private actors, Union and Member States agencies and institutions overlap and (re)negotiate normative, executive, and adjudicative functions. Against this backdrop, this paper examines (i) how cybersecurity exposes the fragility of State power, unable to exert full control over cyberspace; (ii) the emergence and effectiveness of supranational responses at EU level; and (iii) how EU Member States are responding to this crisis. Thus, since the early 2000s, the EU has sought to enhance common resilience and security in cyberspace. Yet, national security remains an exclusive competence of Member States. The result is a (dys)functional dualism whereby the EU fosters regulatory and technical integration through its internal market competences, while States retain exclusive authority over national security. This hybrid arrangement highlights a deep legal-institutional tension and a new vulnerability in Europe's cybersecurity governance, prompting a reconsideration of how sovereignty, coercion, and legality are being redefined in cyberspace.

Keywords: cyberspace, cybersecurity, European Union, national security, turf wars.

1. Introduzione

Nel contesto attuale, in cui rilevanti dimensioni della società e settori del mercato sono sempre più interconnessi e basati su tecnologie digitali, la rilevanza della cybersicurezza ha raggiunto livelli senza precedenti. Nella misura in cui la dipendenza e l'affidamento alle tecnologie digitali si fanno più sistemici e irreversibili, l'esigenza di un maggiore grado di cyberresilienza e cybersicurezza dovrebbe farsi più insistente. Il panorama delle minacce informatiche è da sempre in rapida evoluzione ed espansione – non solo sul piano quantitativo, ma anche su quello qualitativo[1]. Le minacce possono essere di varia origine e, ad

[****] Questo contributo è stato sostenuto dal Progetto SERICS (PE00000014), finanziato dall'Unione Europea – NextGenerationEU attraverso il MUR nell'ambito del PNRR – Missione 4 Componente 2, Investimento 1.3.

[1] ENISA, *ENISA Threat Landscape*, 2025.

un alto livello d'astrazione, possiamo distinguere: i) attacchi di natura criminale comune (ransomware, malware, etc.), di natura politica (campagne di disinformazione) o terroristica (attacchi DDoS, etc.), commissionati o comunque legati ad uno Stato; ii) incidenti causati da calamità naturali ed errori non intenzionali; iii) mancanza di competenze[2]. Sfruttando le già citate interconnessioni delle reti e dei sistemi informativi della società contemporanea, un attacco può paralizzare intere catene di approvvigionamento delle imprese o le infrastrutture critiche di un paese, con pregiudizi per l'intera collettività; sotto altro profilo, può avere risvolti in termini di interferenza con i diritti e le libertà fondamentali delle persone, nella misura in cui, ad esempio, si verifichino violazioni dei dati personali.

Come è noto, il cyberspazio mette in crisi, in modo simultaneo, due categorie classiche del diritto: la sovranità, perché l'esercizio del potere non coincide più con un perimetro territoriale governabile[3]; la normatività, perché una parte decisiva delle sue "regole costitutive"[4] non nasce da leggi emanate da soggetti statuali, bensì da standard tecnici, contratti, policy di piattaforme e scelte architetturali *bottom-up*, in larga misura in mano a privati[5].

In questo quadro, la sicurezza del cyberspazio, o cybersicurezza, diventa una nuova e determinante area del diritto, non tanto per le scelte innovative in termini di approcci regolatori[6] o per l'oggetto e gli obiettivi degli atti giuridici rilevanti, quanto più perché destabilizza il paradigma tradizionale e consolidato della fornitura della sicurezza nello Stato moderno; fondato, cioè, sull'idea che lo Stato è garante esclusivo della sicurezza entro confini definiti e controllabili. La minaccia nel cyberspazio, infatti, è non solo transnazionale, ma anche tecnicamente opaca: spesso non è attribuibile con certezza a un determinato attore ed è mediata da catene globali di soggetti e infrastrutture. Sotto altro profilo, nella misura in cui il cyberspazio è costituito da tecnologie e infrastrutture perlopiù in mano a soggetti privati, la

[2] ENISA, *ENISA Foresight Cybersecurity Threats for 2030 – update*, 2024.
[3] Si vedano, *ex multis,* D.R. Johnson, D. Post, "Law and Borders: The Rise of Law in Cyberspace", *Stanford Law Review,* 48 (1996), 5; C. Ryngaert, "Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts", *German Law Journal*, 24 (2023), 3.
[4] J.R. Searle, *The Construction of Social Reality,* The Free Press, 1995. Sulla tensione tra regole costitutive e regolative, nonché circa l'importanza della strutturazione dell'ambiente alla base delle applicazioni di tecnologie digitali, in particolare dell'intelligenza artificiale (IA), si veda L. Floridi, *Etica dell'Intelligenza Artificiale,* Raffaello Cortina Editore, 2022.
[5] L. Lessig, *Code: and other laws of cyberspace,* Basic Books, 1999; L.A. Bygrave, *Internet Governance by Contract*, Oxford University Press, 2015.
[6] L.A. Bygrave, "The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes", *Computer Law & Security Review*, 56 (2025).

difesa dalle minacce (quindi la sicurezza) è distribuita e l'intervento pubblico è spesso esercitato indirettamente attraverso obblighi imposti agli intermediari e ai detentori delle infrastrutture.

Per far fronte alle molteplici sfide poste alla collettività e al mercato in materia di cybersicurezza, l'Unione europea ha iniziato, sin dai primi anni 2000, a definire una politica in materia di sicurezza delle reti e dei sistemi informativi che si traducesse in misure complementari a quadri giuridici più maturi – e contigui, *ratione materiae* – quali la protezione dei dati personali e il contrasto al cybercrimine[7]. La progressiva emersione di questa nuova area di *policy* a livello di diritto dell'UE (in ragione, come si vedrà, di un livello insufficiente di intervento e consapevolezza, nonché di efficacia della risposta se portata avanti dai singoli Stati) è legata a competenze funzionali, soprattutto con riferimento al funzionamento del mercato interno, e non autonome: i Trattati non riconoscono all'Unione una competenza esplicita nell'ambito della cybersicurezza secondo il principio di attribuzione ex Art. 5 TUE[8]. Al contempo, e solo successivamente, si osserva anche una risposta normativa anche a livello nazionale. L'interventismo regolamentare di Bruxelles si confronta, infatti, con un limite strutturale dell'architettura costituzionale dell'UE: la competenza esclusiva degli Stati membri in materia di sicurezza nazionale[9]. Come ricordato, infatti, interessando l'infrastruttura critica e avendo la potenzialità di compromettere i processi democratici, la minaccia cibernetica diventa inevitabilmente (anche) una questione di sicurezza nazionale.

Ne deriva un "dualismo (dis)funzionale": da un lato, l'UE sviluppa, attraverso la competenza sul mercato interno, un quadro comune per la cybersicurezza e, quindi, cyberresilienza; dall'altro, ogni Stato membro mantiene la piena titolarità nella gestione delle minacce (e quindi anche nella risposta a queste) legate alla difesa dell'interesse nazionale e degli interessi essenziali di sicurezza, categorie giuridico-politiche tipicamente non rigidamente definibili[10]. Questo assetto ibrido riflette una tensione giuridico-istituzionale

[7] Commissione europea, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, COM(2001) 298 definitivo, p. 21.
[8] In base al principio di attribuzione, l'Unione agisce solo entro i limiti delle competenze che le sono conferite dagli Stati membri nei trattati per il raggiungimento degli obiettivi ivi stabiliti. Si veda, *ex multis,* R. Schütze, "EU Competences: Existence and Exercise", in D. Chalmers, A. Arnull (a cura di), *The Oxford Handbook of European Union Law,* Oxford Academic, 2015.
[9] Art. 4, para. 2, Trattato sull'Unione europea.
[10] M. Trybus**,** *Buying Defence and Security in Europe: The EU Defence and Security Procurement Directive in Context*, Cambridge University Press, 2014, pp. 85-135; P. Stompfe, "Foreign Investment Screening in Germany

profonda e svela una vulnerabilità del governo della cybersicurezza nell'Unione europea: l'UE promuove un'integrazione normativa e tecnica finalizzata al mercato, ma gli Stati restano i soli legittimati ad agire come titolari del potere coercitivo in ambito di sicurezza a livello di società.

Da un punto di vista metodologico, la prima questione che l'articolo affronta è se, ed in quale modo, la cybersicurezza determini la crisi del paradigma tradizionale della fornitura della sicurezza nello stato moderno. Quindi, sul piano empirico degli strumenti, l'articolo mette in luce il progressivo slittamento, dagli inizi degli anni 2000, del baricentro del potere normativo effettivo dal livello statale a quello sovranazionale con l'emersione della politica eurounitaria sulla "sicurezza delle reti e dei sistemi informativi". Il quadro delineato consente di passare alla terza e ultima dimensione analitica dell'articolo, di natura normativa, che indaga, da una parte, il ruolo che lo Stato-nazione (in particolare, l'Italia) *cerca* di ritagliarsi e quali siano gli effetti di determinate politiche regolatorie; dall'altra, il ruolo che *dovrebbe* svolgere, alla luce dei tre indicatori di 'crisi' evidenziati nella prossima sezione.

2. La minaccia cibernetica e la crisi del paradigma moderno della sicurezza statuale

Il paradigma moderno della fornitura della sicurezza si consolida attorno a una configurazione concettuale precisa, che trova nel 'modello westfaliano'[11] una prima espressione teorica. In tale modello, la sicurezza è funzione diretta della sovranità suprema dello Stato, che detiene, in via esclusiva, il monopolio della forza legittima, esercitabile entro confini spaziali definiti e giuridicamente controllabili[12]. In Hobbes, la sicurezza costituisce infatti il fondamento ontologico dell'autorità sovrana (sia essa una monarchia o un'assemblea di individui), e anzi, addirittura, la sua ragion d'essere, insieme al mantenimento della pace, in

and France", in S. Hindelang, A. Moberg (a cura di), *YSEC Yearbook of Socio-Economic Constitutions,* Springer, 2020, p. 97. Sul dibattito dottrinale circa l'espressione 'interesse nazionale' nel contesto costituzionale italiano, si veda S. Aru, "La clausola di supremazia statale nel DDL di revisione costituzionale: si scrive 'interesse nazionale', si legge 'indirizzo politico-governativo'", *Costituzionalismo.it*, 1 (2016), pp. 83-87.

[11] D. Armstrong, "The Westphalian conception of international society", in D. Armstrong (a cura di), *Revolution and world order: The revolutionary state in international society,* Oxford University Press, 1993.

[12] D. Philpott, "Sovereignty: An introduction and brief history", *Journal of International Affairs*, 48 (1995), 2, p. 357.

risposta all'insicurezza strutturale dello stato di natura[13].

Il nucleo concettuale di questo paradigma è poi sistematizzato da Weber in termini sociologico-giuridici: la sicurezza si identifica con la produzione e il mantenimento dell'ordine interno, affidate a un apparato istituzionale capace di distinguere tra forza legittima e illegittima[14]. In questo contesto, l'identificazione e il controllo di un territorio geograficamente delimitato sono condizioni giuridiche essenziali che rendono possibile l'esercizio esclusivo, da parte dello Stato, della coercizione e, con essa, la distinzione tra interno ed esterno, tra sicurezza e minaccia.

Un'ulteriore dimensione è data dalla riflessione di Rokkan, che individua nella capacità dello Stato di estrarre risorse dalla società, in particolare attraverso la tassazione, e di convertirle in capacità coercitiva, soprattutto militare, una delle condizioni fondative della statualità moderna[15]. Così, la sicurezza non è solo monopolio giuridico della forza, ma anche la *capacità materiale* di finanziarla, organizzarla e dispiegarla.

La minaccia cibernetica, veicolata attraverso il cyberspazio – "non luogo" in termini geografico-territoriali – mette in crisi l'equilibrio tra queste dimensioni del paradigma classico di sicurezza. Tra le diverse sfide normative poste dal cyberspazio, vale a dire etiche, sociali e giuridiche, è opportuno soffermarsi brevemente su queste ultime, al fine di contestualizzare il quadro analitico volto a sistematizzare le diverse dimensioni epistemologiche del concetto di cybersicurezza nella sezione che segue. In particolare, il proposto impianto analitico considera tre caratteristiche proprie dello spazio cibernetico che sembrano decisive per sostenere la tesi di una crisi del paradigma moderno di sicurezza statuale nel quadro della cybersicurezza: l'extraterritorialità, il primato del settore privato e la difficoltà nell'attribuzione delle responsabilità.

2.1 Cyberspazio, territorialità e sovranità

Il cyberspazio non può essere considerato un'entità giuridica vincolata da confini fisico-

[13] T. Hobbes, *Leviatano*, 1651, Cap. XVIII, para. 6.
[14] M. Weber, *La politica come professione,* Armando editore, 2010, pp. 32-33.
[15] P. Flora, S. Kuhnle, D. Urwin (a cura di), *State Formation, Nation-Building, and Mass Politics in Europe: The Theory of Stein Rokkan*, Oxford University Press, 1999, p. 131.

geografici, su cui insista la sovranità di un soggetto statuale specifico[16]. Questo spazio si compone infatti di diversi livelli, sovrapposti ed interdipendenti[17]: i) livello fisico: comprende l'infrastruttura fisica alla base della rete (cavi sottomarini e terrestri; data center e server farm; satelliti, etc.); ii) livello logico-protocollare: comprende le tecnologie fondamentali per l'interoperabilità delle reti e la connettività (protocolli, es. TCP/IP; sistemi di indirizzamento; root server DNS; standard tecnici, etc.); iii) livello software: traduce l'infrastruttura in capacità operative (sistemi operativi; firmware, etc.); iv) livello applicativo: visibile agli utenti attraverso servizi e applicazioni (piattaforme digitali; servizi cloud, etc.); v) livello dei dati: comprende i flussi dei dati e di informazione; vi) livello sociale: comprende la componente umana e le interazioni sociali nel cyberspazio.

Per quanto il "sogno eccezionalista" di Barlow[18] sia, appunto, rimasto tale, è indubbio che il paradigma di livelli interdipendenti e sovrapposti del cyberspazio è configurato *dinamicamente* dalle interazioni e dai collegamenti tra i suoi livelli e le entità che li costituiscono (reti, protocolli, sistemi, dati, persone), con una struttura definita da queste relazioni più che dalle dimensioni fisiche e territoriali *statiche* del sistema westfaliano[19].

Al tempo stesso, è incontrovertibile che l'ascesa della narrativa sulla c.d. "sovranità digitale"[20] nel dibattito politico rifletta non solo il perdurante potere dello Stato-nazione, ma anche quello di soggetti politici sovranazionali, ad es. l'UE[21]. Così, il cyberspazio è sottoposto dai suoi diversi attori (soprattutto Stati nazione, ma anche gruppi multinazionali e piattaforme,

[16] Cfr. *ex multis* P. Bellanger, "From sovereignty in general to digital sovereignty in particular", *Les Echos*, 54 (2011), 30, p. 3.
[17] B.H. Bratton, *The Stack: On Software and Sovereignty,* The MIT Press, 2015, p. 11: l'autore propone un modello ('the Stack') composto da sei livelli sovrapposti ed interdipendenti (*Earth, Cloud, City, Address, Interface, User*): "each is considered on its own terms and as a dependent layer within a larger architecture, and each is drafted from the superimposed image of the geographic and computational machines we now inhabit and the ones we might yet make".
[18] J.P. Barlow, "A Declaration of the Independence of Cyberspace", *Duke Law & Technology Review*, 18 (2019), 5-7, p. 1: "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather".
[19] F. Pierucci, "Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace", *Digital Society*, 4 (2025), 27, p. 11; S. Couture, S. Toupin, "What does the notion of 'sovereignty' mean when referring to the digital?", *New Media & Society,* 21 (2019), 10, p. 2311.
[20] Concetto appositamente elusivo, sfruttato nelle narrative politiche degli Stati per legittimare pretese di influenze strategiche sullo spazio digitale, si veda F. Pierucci, "Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace", cit., pp. 5-6; cfr. L. Floridi, "The fight for digital sovereignty: What it is, and why it matters, especially for the EU", *Philosophy & Technology*, 33 (2020), 3.
[21] S. Couture, S. Toupin, "What does the notion of 'sovereignty' mean when referring to the digital?", cit.

fino agli user stessi, seppur con capacità e in ordini di grandezza diversi) a processi continui di de-territorializzazione e ri-territorializzazione[22], fino ad arrivare a tentativi (più o meno riusciti) di estendere la propria sovranità in altrui territori e giurisdizioni, come nel caso della politica digitale dell'UE, ad iniziare dal regolamento generale sulla protezione dei dati personali oppure ancora nel caso della sorveglianza di massa – con conseguente invasione di diritti e libertà fondamentali, come dimostrato da Stati autoritari e non[23].

In questo contesto, la sicurezza, nelle sue molteplici dimensioni, perde il suo tradizionale ancoraggio territoriale. L'elemento geografico, che nella dimensione analogica-cinetica è ostacolo e freno ad attività che minino la sicurezza di un soggetto statuale, delle sue infrastrutture, dei suoi consociati (ad esempio, attività terroristiche, di spionaggio, di sabotaggio o di sorveglianza), è annullato nella dimensione cibernetica. Un "asset" connesso è potenzialmente raggiungibile da qualsiasi parte del mondo. Al tempo stesso, i danni che possono derivare da attacchi nella dimensione digitale sono considerevoli, soprattutto quando le infrastrutture critiche di un Paese diventano bersaglio di attacchi coordinati da altri soggetti statuali[24]. Non a caso, nell'ambito del diritto internazionale, sta emergendo un consenso "volto a subordinare la qualificazione di un'operazione informatica quale uso illecito della forza armata alle conseguenze che essa produce"[25].

2.2 Dipendenza da fornitori privati ed esteri e vulnerabilità strategiche

Il cyberspazio frammenta anche il tradizionale monopolio in capo allo Stato delle *strutture* della sicurezza. Già nel 2001, la Comunicazione della Commissione europea sulla sicurezza delle reti e dei sistemi informativi riconosceva che la proprietà e la gestione delle reti fossero soprattutto private[26]. La prima Strategia europea per la cybersicurezza del 2013 recepisce quindi questo dato fattuale constatando come la riuscita di qualsiasi iniziativa legata alla sicurezza del cyberspazio sarebbe necessariamente dovuta passare attraverso il

[22] D. Lambach, "The Territorialization of Cyberspace", *International Studies Review*, 22 (2020), pp. 483-484.
[23] J. Ruohonen, "The treachery of images in the digital sovereignty debate", *Minds and Machines*, 31 (2021), 3.
[24] Su tutti, basti pensare agli attacchi informatici subiti dall'Estonia (2007) e dalla Costa Rica (2022).
[25] G. Gabrielli, "La governance internazionale della cybersicurezza: cyber attacchi contro infrastrutture critiche nella prospettiva dello *jus ad bellum*", in R. Brighi, G. Adinolfi (a cura di), *Governare la sicurezza degli (eco)sistemi cyberfisici: Regolamentazione, diritti e politiche*, Giappichelli, 2025, p. 94.
[26] Commissione europea, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, cit., p. 8.

riconoscimento del "ruolo motore" del settore privato, fermo restando il "ruolo decisivo" degli Stati nella garanzia della libertà e della sicurezza anche in questa dimensione[27].

La topologia della rete Internet globale, elemento centrale e preponderante del cyberspazio, è determinata dai diversi attori privati che detengono la proprietà delle infrastrutture di rete necessarie alla prestazione dei diversi servizi (*internet service provider*, *content delivery networks*, *cloud services providers*). Ruiz e Barnett mostrano che circa 16 gruppi di imprese, con sede in 7 paesi, costituiscono il centro della rete globale[28].

Nel contesto dell'analisi sulla (pretesa, e gli sforzi di) sovranità statuale sull'infrastruttura fisica del cyberspazio, è necessario considerare non solo le relazioni internazionali tra Stati[29], ma anche (e soprattutto) le interazioni tra Stati e imprese private: ad esempio, con riferimento specifico ai cavi sottomarini che permettono la connettività delle telecomunicazioni globali, il concetto di sovranità digitale "encompasses the authority of nations to dictate the routes and locations where cables are laid within their territories, establish standards for the cables and the data transmitted through them, and ensure robust protection to sustain internet provision and safeguard the privacy of transmitted data"[30]. Dal momento che la maggior parte di questa infrastruttura è di esclusiva proprietà del settore privato[31], le grandi multinazionali esercitano un grado di influenza maggiore sulle politiche statali, con conseguenti impatti sulla sovranità[32].

Peraltro, l'affidamento a soggetti esteri per la fornitura di servizi essenziali di connettività pone seri problemi non solo, come visto, in termini di sovranità e giurisdizione, ma anche di vulnerabilità strategica. Infatti, gli Stati possono esercitare un controllo più o meno elevato sulle imprese che forniscono servizi Internet attraverso forme di partecipazione statale, la regolamentazione e la pressione politica. Pertanto, i soggetti statuali che dipendono

[27] Commissione europea e Alta rappresentante dell'UE per gli Affari esteri e la Politica di sicurezza, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, JOIN(2013) 1 definitivo, p. 2.
[28] J.B. Ruiz, G.A. Barnett, "Who owns the international Internet networks?", *The Journal of International Communication*, 21 (2015), 1.
[29] La Convenzione ONU sul diritto del mare (Convenzione di Montego Bay) stabilisce *inter alia* la libertà dell'alto mare per tutti gli Stati ed include la libertà di posa di cavi sottomarini. Altre regole vigono per la posa di cavi sulla piattaforma continentale (Art. 79) e nella zona economica esclusiva (Art. 58).
[30] A. Ganz *et al.*, "Submarine cables and the risks to digital sovereignty", *Minds and Machines,* 34 (2024), 31, p. 3.
[31] J. Sherman, "Cyber Defense across the Ocean Floor: the Geopolitics of Submarine Cable Security", *Atlantic Council*, 2021, p. 9: al dicembre 2020, il 59% (279 su 475) dei cavi sottomarini ha proprietà e gestione private.
[32] A. Ganz *et al.*, "Submarine cables and the risks to digital sovereignty", cit., p. 5: gli Autori citano il caso Google-Nigeria del 2021.

esclusivamente o in larga parte da fornitori privati e/o altri Stati, prendono atto che la sicurezza (non solo digitale, ma anche fisica dell'infrastruttura) è assicurata da altri e, allo stesso tempo, valutano i rischi derivanti da una serie eterogenea di minacce: di sicurezza fisica, con riferimento sia ad attività dolose di sabotaggio che ad incidenti accidentali; e cyber, come nel caso della sorveglianza e del controllo sui dati, personali e non. Alla luce dell'importanza del settore privato nel cyber spazio, soggetti politici sia a livello nazionale che sovranazionale hanno progressivamente promosso modelli di governance multi-stakeholder cooperativa come le partecipazioni pubblico-privato (PPPs), ad esempio nel contesto della protezione dell'infrastruttura critica[33].

2.3. Anonimato: difficoltà di attribuzione della responsabilità ed *enforcement*

Le caratteristiche strutturali del cyberspazio suesposte complicano la relazione, consolidata nel mondo analogico, tra coercizione, responsabilità e capacità materiale di applicazione delle norme (*enforcement*). Tra le diverse tipologie di minacce cibernetiche, quelle che più interessano la presente disamina sono gli attacchi e gli incidenti che innescano la risposta coercitiva dello Stato, sia sul fronte penalistico sia su quello della difesa. Per quanto risposte decise siano giunte sin dalle prime fasi della cd. "rivoluzione digitale"[34] sul piano del diritto internazionale[35], sovranazionale[36] e nazionale[37] in materia di contrasto alla criminalità informatica, l'approccio di stampo penalistico, caratterizzato cioè dall'intervento dell'autorità pubblica una volta che si sia commesso il fatto illecito (penale), si è dimostrato almeno in parte inefficace, dal momento che fatica ad assolvere il suo compito principale: trovare il responsabile da perseguire, processarlo ed (eventualmente) ottenere una condanna.

In primo luogo, i protocolli di rete privilegiano l'instradamento efficiente dei pacchetti di

[33] F. Cappelletti, L. Martino, "Achieving Robust European Cybersecurity through Public–Private Partnerships: Approaches and Developments", *EU Policy Review*, 1 (2021); F. Serini, "Collective cyber situational awareness in EU. A political project of difficult legal realisation?", *Computer Law & Security Review*, 55 (2024), p. 6.
[34] L. Floridi, *La quarta rivoluzione: come l'infosfera sta cambiando il mondo,* Raffaello Cortina editore, 2017.
[35] La Convenzione di Budapest (CoE) sulla criminalità informatica prevede la criminalizzazione di alcune condotte, accesso illegale, all'interferenza nei dati e nei sistemi alla frode informatica e alla diffusione di materiale pedopornografico.
[36] Direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione che sostituisce la decisione quadro 2005/222/GAI del Consiglio.
[37] Ad es., nel contesto italiano, si veda la L. 547/1993.

dati, non l'autenticazione della fonte. A ciò si aggiunge l'uso sistematico, da parte degli attori della minaccia, di tecniche di anonimizzazione e offuscamento, quali l'*IP spoofing*, le reti di *proxy*, le VPN e i servizi di *onion routing*, che consentono di mascherare o moltiplicare i punti di origine apparente dell'attacco. In secondo luogo, molti attacchi sono condotti tramite infrastrutture intermediarie compromesse, come *botnet* costituite da dispositivi di proprietari ignari, che fungono da vettori dell'azione offensiva e complicano la ricostruzione della responsabilità[38].

Un'ulteriore criticità deriva dalla dimensione transnazionale delle reti e dalla frammentazione delle fonti di prova digitale: i log di sistema, indispensabili per la ricostruzione tecnica degli eventi, sono distribuiti tra una pluralità di soggetti privati, collocati in giurisdizioni diverse, soggetti a regimi di conservazione eterogenei. In questo contesto, la Convenzione di Budapest è stata e rimane un quadro giuridico essenziale per ampliare e accelerare l'assistenza giudiziaria reciproca tra le diverse autorità nazionali. L'accesso transfrontaliero alle prove digitali è infatti una questione urgente nel 55% delle indagini e dei procedimenti penali[39].

Se, a livello regionale, l'Unione europea, nel corso degli ultimi tre decenni, ha sviluppato iniziative legislative per rafforzare meccanismi di cooperazione tra le diverse autorità nazionali, attraverso, ad esempio quadri di scambio di informazioni anche e soprattutto tramite la cooptazione del settore privato[40], anche a livello internazionale si è cercato di rispondere in concreto a queste sfide. Da un lato, la Convenzione di Budapest ha adesso un secondo protocollo sulla cooperazione rafforzata che mira proprio a rafforzare l'efficacia dell'assistenza giudiziaria reciproca; dall'altro, nel dicembre 2024, l'Assemblea Generale dell'ONU ha adottato la Convenzione ONU contro il cybercrimine[41].

Sebbene indubbiamente importanti, queste iniziative non sembrano affrontare la questione fondamentale dell'*enforcement*. Peraltro, sul piano europeo, una larga parte degli attacchi e delle minacce proviene da paesi terzi[42]. Così, come già avviene a livello internazionale, anche

[38] W.E. Boebert, "A Survey of Challenges in Attribution", *National Academies*, Atti del *Workshop on Deterring Cyberattacks*, The National Academies Press, 2010, p. 43 ss.
[39] Y. Miadzvetskaya, R. Wessel, "The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox", *European Papers,* 7 (2022), 1, p. 424.
[40] N. Vavoula, "The Future of Digitalisation in EU Law Enforcement: Enhanced Exchanges of Personal Data, Privatisation and Algorithmisation", *European Papers,* 10 (2025), 3.
[41] Risoluzione ONU 79/243.
[42] ENISA, *ENISA Threat Landscape*, cit., p. 36 ss.

il successo dei diversi quadri europei dipende in gran parte dalla volontà politica dei paesi che dovrebbero identificare, arrestare e consegnare i responsabili affinché siano puniti. Tuttavia, l'UE non dispone di procedure per l'attribuzione della responsabilità degli attacchi informatici ai paesi terzi, poiché non esiste la volontà politica di stabilire quadri comuni di attribuzione, decisione politica sovrana riservata agli Stati membri[43]: le sanzioni all'interno del quadro *Cyber Diplomacy Toolbox*[44] sono misure mirate rivolte a individui, gruppi o aziende e non portano, *stricto sensu,* all'attribuzione di responsabilità a uno Stato, ancorché secondo autorevole dottrina queste misure individuali possano essere lette come un'attribuzione *indiretta* alla responsabilità degli Stati[45].

Al tempo stesso, i gruppi cybercriminali più attivi e potenti, non solo trovano rifugio in Stati che tollerano il loro operato, ma, sempre più spesso, diventa difficile nella pratica distinguere tra attacchi motivati esclusivamente dal profitto senza l'intromissione di apparati statali e più vaste cyber operazioni parte di strategie di guerra ibrida coordinate da agenzie governative e di intelligence al fine di conseguire obiettivi geopolitici legati all'interesse nazionale[46]. Ne consegue che il cyberspazio porta anche all'offuscamento e sfumatura del confine, chiaramente distinguibile nella dimensione analogica, tra crimine e atto di guerra[47].

L'inefficacia degli strumenti giuridici per l'accesso e la raccolta di prove digitali ha, a sua volta, comportato conseguenze giuridiche indesiderabili che, in modo non sorprendente, si legano alla prima dimensione analitica presa in esame: i singoli Stati hanno iniziato a rivendicare la giurisdizione extraterritoriale in materia di cybercrimini, obbligando le aziende soggette alla loro giurisdizione a concedere l'accesso ai dati indipendentemente dall'ubicazione dei server[48]. Questa soluzione ha poco a che vedere con il quadro internazionale e sovranazionale che mira a conciliare la sovranità nazionale con la necessità di cooperazione[49].

---

[43] Cons. 9, Decisione (PESC) del Consiglio (PESC) 2019/797.
[44] Decisione (PESC) del Consiglio (PESC) 2019/797 e Regolamento (UE) 2019/796 del Consiglio.
[45] Y. Miadzvetskaya, R. Wessel, "The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox", cit., pp. 434-435.
[46] L. Lonardo (a cura di), *Addressing Hybrid Threats: European Law and Policies,* Edgar Elgar, 2024.
[47] A. Missiroli, "From hybrid warfare to 'cybrid' threats – and back? Concepts, challenges, responses", in L. Lonardo (a cura di), *Addressing Hybrid Threats: European Law and Policies,* cit., p. 44.
[48] Y. Miadzvetskaya, R. Wessel, "The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox", cit., p. 424.
[49] P. Arnell, B. Faturoti, "The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted", *International Review of Law, Computers and Technology*, 37 (2023), 1, p. 29 ss.

Come ricordato nel preambolo del regolamento UE "Cybersecurity Act" del 2019, per rispondere efficacemente a cyberattacchi e minacce, intrinsecamente transfrontalieri, sono necessarie capacità effettive e coordinate di risposta e di gestione delle crisi a livello di Unione, sulla base di apposite politiche e strumenti di più ampia portata per la solidarietà europea e l'assistenza reciproca, ancorché tali competenze e le relative risposte politiche siano prevalentemente nazionali[50].

2.4 Una conclusione preliminare

Le tre caratteristiche strutturali del cyberspazio analizzate in questa sezione contribuiscono a indebolire la capacità degli Stati di esercitare in modo autonomo ed efficace le funzioni classiche di prevenzione e risposta nella dimensione cibernetica. Tali elementi non determinano, evidentemente, una perdita della titolarità statale del potere coercitivo, che resta saldamente ancorata agli ordinamenti nazionali, ma ne riducono significativamente l'efficacia operativa quando la regolamentazione degli aspetti di cybersicurezza è confinata a un perimetro esclusivamente nazionale. Il problema centrale affrontato dal presente contributo si colloca proprio nello scarto tra la competenza formale e l'efficacia delle politiche e degli strumenti.

Nelle sezioni che seguono, il saggio mette in luce tale "dualismo disfunzionale" della governance della cybersicurezza in Europa, inteso come la coesistenza strutturalmente asimmetrica di due piani regolatori distinti, quello sovranazionale e quello nazionale, nei quali l'Unione europea, pur priva di una competenza esplicita in materia di cybersicurezza, interviene sui presupposti materiali, tecnici e organizzativi di questa attraverso strumenti regolatori fondati sulle competenze del mercato interno[51]. Si vedrà, in particolare, se ed in che misura l'azione a livello sovranazionale tenda a rivelarsi più incisiva sul piano della prevenzione e della resilienza rispetto alle risposte statali tradizionali.

[50] Cons. 5, Regolamento (UE) 2019/881.
[51] In altri termini, si veda M. Matassa, *La sicurezza cibernetica come funzione pubblica,* FrancoAngeli, 2025. L'autore sviluppa un interessante quadro teorico che vedrebbe la cybersicurezza come una funzione pubblica multilivello composta da tre cerchi concentrici (p. 74-75). In questo senso, si sottolinea come "l'integrazione progressiva delle funzioni di 'sicurezza nazionale' (nel contesto interno) e di 'tutela del mercato dell'Unione' (nel contesto UE) [abbia] dato origine a una funzione composita che non si presta a essere rappresentata attraverso la somma di ogni sua singola componente" (p. 88).

La tensione tra titolarità del potere coercitivo ed efficacia regolatoria è analizzata attraverso l'esame del caso italiano. Gli Stati membri, forti della competenza esclusiva in materia di sicurezza nazionale e della tradizionale legittimazione all'uso della coercizione in risposta a minacce alla sicurezza, mostrano una persistente refrattarietà, da una parte, ad estendere il coinvolgimento dell'UE nelle attività operative della cybersicurezza – soprattutto, gestione delle crisi, condivisione delle informazioni e segnalazione degli incidenti[52] (sezione 3) e, dall'altra, a rinunciare all'adozione di strumenti normativi autonomi, anche quando tali interventi risultino ridondanti o, addirittura, disallineati rispetto al quadro eurounitario (sezione 4).

3. La governance multi-stakeholder e multi-livello della cybersicurezza nell'UE

Agli inizi degli anni 2000, la Commissione europea propone una visione strategica per una politica comunitaria sulla sicurezza delle reti e dei sistemi informativi che avrebbe portato miglioramenti ad un mercato caratterizzato da 'fallimenti', ove cioè gli operatori non riescono a generare investimenti sufficienti nelle tecnologie e nella cultura della sicurezza a causa di diverse esternalità negative (es., mancanza di strumenti di responsabilità civile per i danni cagionati dal comportamento degli operatori in relazione alla sicurezza; asimmetrie informative in relazione a rischi e benefici)[53].

Secondo la Commissione, il fatto che le reti e i sistemi informativi fossero in larga parte in mano ai privati e implicassero comunicazioni (e infrastrutture) transfrontaliere (sezione 2) "[avrebbe limitato] la possibilità delle autorità nazionali di intervenire sul livello di sicurezza delle comunicazioni elettroniche di cittadini ed imprese. Ciò non significa tuttavia che il settore pubblico non abbia più alcun ruolo da svolgere in questo campo"[54]. Infatti, fu il combinato disposto della globalizzazione dei proprietari dell'infrastruttura del cyberspazio, della liberalizzazione dei mercati delle reti e dei sistemi informativi e dell'interconnessione tecnologica dell'infrastruttura a rendere la sicurezza un aspetto dell'offerta di mercato.

[52] S. Backman, "Risk vs. threat-based cybersecurity: the case of the EU", *European Security,* 32 (2023), 1, p. 99.
[53] Commissione europea, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, cit., pp. 19-21.
[54] *Ibid.*, p. 8.

Le suesposte imperfezioni del mercato, unitamente all'aumento della minaccia cibernetica, per sua natura transnazionale, hanno reso manifesta l'inefficacia di una risposta normativa sul piano nazionale, spingendo l'allora Comunità europea a pensare a un quadro normativo orizzontale per la sicurezza delle reti e dell'informazione, superando così la frammentazione delle misure di sicurezza tra diversi quadri giuridici, in particolare in materia di telecomunicazioni, protezione dei dati personali e contrasto al crimine informatico.

Una delle prime iniziative europee in materia di cybersicurezza è la creazione dell'ENISA, l'Agenzia europea per la sicurezza delle reti e dell'informazione (ora, semplicemente, Agenzia dell'Unione europea per la cybersicurezza), nel 2004, con diversi obiettivi: condurre analisi dei rischi, fornire consulenza sulle questioni in materia di sicurezza delle reti e dell'informazione, facilitare la cooperazione e contribuire alla "sensibilizzazione" in questo campo, nonché monitorare gli standard e il contributo agli sforzi dell'UE per cooperare a livello internazionale[55]. Tuttavia, non solo l'ENISA ricevette inizialmente mandato temporaneo, ma la base giuridica adottata per la sua fondazione – l'Articolo 95 Trattato CE, antesignano dell'Art. 114 TFUE sul funzionamento del mercato interno – fu addirittura contestata dal Regno Unito, che adì la Corte di Giustizia[56].

Inizialmente, l'Agenzia faticò a imporsi come autorità epistemica, anche perché non disponeva di poteri formali di governo né di capacità regolamentare: "many regulating bodies opposed the EU's aspiration to be a 'super-regulator' in telecommunications, and ENISA was seen as part of this problem"[57]. Per quanto il mandato dell'ENISA fosse stato rinnovato altre due volte e si iniziassero ad intravedere tentativi regolatori, ancorché frammentati, attraverso strumenti giuridicamente vincolanti[58], la vera svolta della *governance* europea della cybersicurezza arriva solo nel 2013, quando l'Unione si dota di una Strategia per la sicurezza delle reti e dei sistemi informativi[59].

Con questo decisivo passo, la 'cybersicurezza' diventa, a tutti gli effetti, una politica

[55] Regolamento (CE) 460/2004.
[56] Corte di giustizia dell'Unione europea (Grande Sezione), Causa C-217/04, *Regno Unito v. Parlamento e Consiglio,* 2 maggio 2006.
[57] M. Dunn Cavelty, M. Smeets, "Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority", *Journal of European Public Policy,* 30 (2023), 7, pp. 1337-1338.
[58] Decisione quadro 2005/222/GAI del Consiglio del 24 febbraio 2005 relativa agli attacchi contro i sistemi di informazione.
[59] Commissione europea e Alta rappresentante dell'UE per gli Affari esteri e la Politica di sicurezza, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, cit.

dell'Unione[60]: vengono dispiegate azioni e strumenti intorno a cinque priorità strategiche, non solo per preservare il corretto funzionamento del mercato, ma anche con ripercussioni sul piano della difesa nel quadro della Politica di sicurezza e di difesa comune (PSDC) e della politica estera e di sicurezza comune, evidenziando le ambizioni di rafforzare l'autorità politica dell'UE e le capacità (sovra)statali in materia di cybersicurezza.

Coerentemente con le sfide normative viste nella sezione precedente, l'approccio di *governance* della Commissione è *multi-stakeholder*[61]: da una parte, il settore privato dovrà continuare a svolgere un ruolo motore nella costruzione e nella gestione del cyberspazio[62]; dall'altra, il settore pubblico, incapace di fornire il bene pubblico della (cyber)sicurezza da solo, dovrà raggiungere un buon bilanciamento tra necessità di introdurre nuovi obblighi di sicurezza, trasparenza e responsabilità e, dall'altra, evitare un intervento nel mercato indebitamente intrusivo, dal momento che ciò che lo Stato mira a proteggere per ragioni di sicurezza nazionale costituisce anche il fondamento della competitività e della prosperità di una Nazione[63].

La direttiva (UE) 2016/1148 (direttiva NIS), recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, unanimemente riconosciuta come il primo atto giuridico dell'Unione sulla cybersicurezza *in senso stretto*[64], è la principale misura legislativa che implementa la Strategia, quantomeno con riguardo alla prima priorità strategica, vale a dire, migliorare la cyber resilienza.

Ad un alto livello, la direttiva impone a operatori di servizi essenziali e fornitori di servizi digitali obblighi organizzativi e tecnici di gestione del rischio e obblighi di notifica degli incidenti, accompagnati da meccanismi di cooperazione (Gruppo di cooperazione NIS, rete CSIRTs), in cui sono coinvolte autorità nazionali degli Stati membri, che prescindono, in larga misura, dall'identificazione certa dell'autore di un eventuale attacco. Non

[60] G.G. Fuster, L. Jasmontaite, "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights", in M. Christen, B. Gordijn, M. Loi (a cura di), *The Ethics of Cybersecurity*, Springer, 2020, p. 98.
[61] Una presa d'atto rinvenibile anche a livello nazionale: ad es., la Germania riconosce esplicitamente che la cybersicurezza è un'attività condivisa tra più attori: Governo federale tedesco, *Robust. Resilient. Sustainable. Integrated Security for Germany: National Security Strategy*, 2024, p. 59.
[62] Commissione europea e Alta rappresentante dell'UE per gli Affari esteri e la Politica di sicurezza, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, cit., pp. 3-4.
[63] M. Dunn Cavelty, F. Egloff, "The Politics of Cybersecurity", *St Antony's International Review,* 15 (2019), 1, p. 42.
[64] Cons. 15, Cybersecurity Act.

sorprendentemente[65], la direttiva NIS ha per base giuridica l'articolo 114 TFUE, "successore" dell'articolo 95 CE utilizzato per l'istituzione dell'ENISA, avente per oggetto il ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri relative all'instaurazione e al funzionamento del mercato interno. Coerentemente, la direttiva NIS parte dall'assunto che la sicurezza e l'affidabilità delle reti, dei sistemi e dei servizi informativi siano innanzitutto necessarie "per le attività economiche e sociali e in particolare ai fini del funzionamento del mercato interno"[66].

Nel 2017, poi, la Commissione e l'Alto Rappresentante aggiornano la politica dell'UE in materia di cybersicurezza con una seconda Strategia[67]. In questo contesto, la cybersicurezza viene sempre più rappresentata come una sfida comune, poiché ad essere minacciato non è solo il mercato unico digitale, ma anche "il funzionamento stesso delle nostre democrazie, le nostre libertà e i nostri valori"[68]. Gli sforzi legislativi si concentrano nuovamente sulla priorità strategica del rafforzamento della cyber resilienza: il Regolamento UE 2019/881 (c.d. *Cybersecurity Act*), da una parte, consolida il ruolo dell'ENISA, attraverso un mandato permanente, nuovi obiettivi, compiti e poteri; dall'altra, istituisce il quadro europeo di certificazione della cybersicurezza per sostenere la crescita del mercato unico della cybersicurezza. Anche in questo caso, la sicurezza viene spostata a monte dell'incidente (indipendentemente dall'eventuale origine malevola), verso standard tecnici e livelli di affidabilità verificabili, tipici di un modello anticipatorio basato sulla certificazione – che però rimane strumento di diritto privato di natura volontaria. Allo stesso tempo, gli Stati membri hanno sottolineato il ruolo dell'Agenzia come soggetto di supporto alla cooperazione operativa su richiesta degli Stati membri, anziché come esecutore di compiti operativi[69].

Quindi, nel dicembre 2020 viene pubblicata la terza Strategia dell'Unione per la

[65] Peraltro, le scelte regolatorie fatte dal legislatore europeo in materia di cybersicurezza si allineano ad un trend contrassegnato dalla sussunzione di più settori alla competenza dell'Unione in materia di mercato interno: si veda sul punto F. Casolari, F. Ferri, S. Villani, "La costituzionalizzazione della cybersicurezza nell'ordinamento dell'Unione europea", in R. Brighi, G. Adinolfi (a cura di), *Governare la sicurezza degli (eco)sistemi cyberfisici: Regolamentazione, diritti e politiche*, cit., p. 32; cfr. S. Weterhill, *The Internal Market as a Legal Concept*, Oxford University Press, 2016.
[66] Cons. 1, Direttiva NIS.
[67] Commissione europea e Alto Rappresentante dell'UE per gli Affari esteri e la Politica di sicurezza, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, JOIN(2017), 450 final.
[68] *Ibid.*, p. 2.
[69] S. Backman, "Risk vs. threat-based cybersecurity: the case of the EU", cit., p. 98.

cybersicurezza[70]. Le tre aree di intervento in cui vengono proposte azioni e misure a livello normativo, di investimento e politico ricalcano ad un alto livello quelle già identificate nelle precedenti Strategie: resilienza e gestione del rischio restano centrali, ma vengono integrate esplicitamente nella triade "resilienza, sovranità tecnologica e leadership", insieme al rafforzamento delle capacità operative di prevenzione, dissuasione e risposta, e alla proiezione esterna dell'UE per un cyberspazio globale e aperto.

In particolare, nell'ambito della prima area, vengono inquadrate diverse proposte sul piano legislativo, ad iniziare dal disegno di revisione della direttiva NIS, che dà luogo alla direttiva UE 2022/2555 (NIS2). La NIS2 conferma la logica di gestione del rischio, estendendo il perimetro e riducendo la discrezionalità degli Stati membri nell'identificazione dei soggetti NIS mediante l'introduzione di un criterio dimensionale. Infatti, in un dominio transnazionale come quello della cybersicurezza, l'eterogeneità delle misure di recepimento nazionali può diventare un moltiplicatore di vulnerabilità.

Inoltre, la NIS2 contribuisce a dare rilevanza sovranazionale alla gestione del rischio, delle minacce e degli incidenti, attraverso un complesso reticolato di quadri coordinati di cooperazione a livello sovranazionale (es., EU-CyCLONe), e internazionale (accordi internazionali ex art. 17 NIS2); tramite l'incoraggiamento della condivisione di informazioni pertinenti (es., minacce, indicatori di compromissione, tecniche e procedure, ecc.) tra soggetti NIS e delle pratiche di divulgazioni coordinate delle vulnerabilità (tramite l'istituzione di una banca dati europea delle vulnerabilità mitigate) al fine di aumentare il livello collettivo di cybersicurezza prevenendo così incidenti. Sempre sul fronte della prevenzione, la direttiva NIS2 rafforza il previgente quadro di misure tecniche, operative e organizzative di gestione del rischio, e notifica degli incidenti da parte dei soggetti NIS2. In parallelo, strumenti settoriali come il Regolamento (UE) 2022/2554 (DORA) replicano lo stesso approccio di gestione del rischio nel settore finanziario, costruendo la "resilienza operativa digitale" come dovere organizzativo permanente e verificabile.

Tuttavia, anche nella traiettoria della direttiva NIS2 è visibile il limite istituzionale del progetto di 'europeizzazione' della cybersicurezza, mai del tutto completato[71].

[70] Commissione europea e Alto Rappresentante dell'UE per gli Affari esteri e la Politica di sicurezza, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, JOIN(2020), 18 final.
[71] F. Serini, "Collective cyber situational awareness in EU. A political project of difficult legal realisation?", cit., p. 12.

L'armonizzazione avanza entro i limiti previsti dai Trattati: l'UE agisce soprattutto sulla base della competenza sul funzionamento del mercato interno e attraverso una crescente produzione di standard, mentre l'operatività resta politicamente presidiata dagli Stati. La NIS2 rafforza la rilevanza sovranazionale della gestione del rischio attraverso un reticolato cooperativo (EU-CyCLONe, accordi di condivisione delle informazioni, divulgazione coordinata vulnerabilità, banca dati europea delle vulnerabilità gestita dall'ENISA), ma le frizioni tra Stati e istituzioni UE emergono nei gangli tipicamente connessi alla sicurezza nazionale: esclusione dall'ambito di applicazione dei soggetti operanti nei settori della difesa, della sicurezza nazionale e nelle attività di contrasto; gestione operativa degli accordi di condivisione delle informazioni in capo ai CSIRT nazionali; ENISA relegata ad un ruolo di assistenza e fornitura di orientamenti; ruolo di osservatore della Commissione nella rete EU-CyCLONe, a meno che l'incidente su vasta scala non abbia (probabilità di avere) un impatto significativo sui servizi ed attività in ambito NIS; notifica degli incidenti significativi alle autorità nazionali competenti.

Ancorché non direttamente previsto dalla terza Strategia, il Regolamento (UE) 2024/2847 (*Cyber Resilience Act*, CRA) estende la logica di gestione anticipatoria del rischio di cybersicurezza ai c.d. "prodotti con elementi digitali", introducendo requisiti obbligatori di cybersicurezza per i fabbricanti, che riguardano la pianificazione, la progettazione, lo sviluppo e la manutenzione di tali prodotti, da rispettare in ogni fase del loro ciclo di vita[72]. Senza il rispetto di questi "requisiti essenziali", il prodotto non può essere immesso sul mercato, in linea con i principi e meccanismi della legislazione armonizzata in materia di sicurezza dei prodotti[73]. Con il CRA, il legislatore europeo interviene nel punto in cui la privatizzazione del cyberspazio è più strutturale: la produzione e l'immissione sul mercato di hardware e software.

Anche nel contesto del CRA, tuttavia, si sono segnalati significativi 'conflitti di competenza': se la proposta iniziale della Commissione imponeva ai fabbricanti di notificare unicamente all'ENISA qualsiasi vulnerabilità attivamente sfruttata contenuta nel prodotto con

[72] Per una panoramica completa degli approcci regolatori del CRA, si permetta di rinviare a: P.G. Chiara, "Gli approcci regolatori del regolamento (UE) in materia di (cyber)sicurezza dei prodotti: il Cyber Resilience Act", in R. Brighi, G. Adinolfi (a cura di), *Governare la sicurezza degli (eco)sistemi cyberfisici: Regolamentazione, diritti e politiche,* cit.
[73] Commissione europea, *La guida blu all'attuazione della normativa UE sui prodotti 2022*, 2022/C 247/01.

elementi digitali, gli Stati membri hanno ottenuto, nel contesto del 'trilogo', che i destinatari di tale notifica fossero anche i CSIRT nazionali[74]. Oltre a soddisfare esigenze di natura tecnico-operativa (ENISA non ha funzioni *stricto sensu* di risposta), tale scelta riflette indubbiamente una questione di controllo su informazioni ad alto valore strategico con implicazioni per la sicurezza nazionale[75].

Il rafforzamento della cyber resilienza dell'Unione non si limita ad obblighi di gestione del rischio di cybersicurezza per servizi (NIS2) e prodotti (CRA), ma include meccanismi più articolati di capacità a livello sovranazionale: il Cyber Solidarity Act (CSoA), regolamento (UE) 2025/38, mira a potenziare la capacità dell'UE di rilevare, prevenire e rispondere a incidenti di cybersicurezza significativi o su vasta scala, attraverso la creazione di un sistema europeo di allerta per la cybersicurezza, basato su una rete di "poli informatici" costituiti dagli Stati su base volontaria ma finanziati dall'UE; un meccanismo per le emergenze di cybersicurezza, che istituisce la "riserva per la cybersicurezza", ossia fornitori privati di fiducia che possano offrire servizi di risposta su richiesta degli Stati colpiti da incidenti su larga scala; un meccanismo europeo di riesame degli incidenti, volto a trarre insegnamenti dagli incidenti significativi.

Il perimetro d'azione dei meccanismi del CSoA, per quanto azionabili su base volontaria dagli Stati, inevitabilmente interseca con le prerogative degli Stati membri in materia di sicurezza nazionale; peraltro, l'estensione dei servizi della 'cyber riserva' alle istituzioni europee è anche stato letto come un ulteriore passo verso una "europeizzazione" della sicurezza, quel processo, cioè, attraverso cui l'Unione si dota di strumenti propri di cyber difesa e resilienza (già iniziato con l'istituzione del CERT-EU nel 2011), "che operano in parallelo e non in sostituzione delle prerogative nazionali, rafforzando così la tutela dell'integrità istituzionale e della sovranità europea"[76].

Del resto, già nella Strategia dell'UE sulla sicurezza del 2020 la Commissione tratteggiava chiaramente l'anacronismo di approcci isolati di sicurezza nazionali:

[74] J. Ruohonen, P. Timmers, "Vulnerability Coordination under the Cyber Resilience Act", *Applied Cybersecurity & Internet Governance*, 4 (2025), 1.
[75] Si legga in tal senso il proposto regolamento delegato che specifica i termini e le condizioni per l'applicazione dell'Art. 16, para. 2 CRA, che permette, in circostanze eccezionali e per motivi legati alla cybersicurezza, al CSIRT designato che riceve per primo la notifica di ritardarne la diffusione agli altri CSIRT europei in cui il prodotto è stato messo a disposizione.
[76] F. Casolari, F. Ferri, S. Villani, "La costituzionalizzazione della cybersicurezza nell'ordinamento dell'Unione europea", cit., p. 45.

> I cittadini non possono essere protetti solo dagli Stati membri che agiscono singolarmente. Oggi più che mai dobbiamo far leva sui nostri punti di forza per lavorare insieme e l'UE è in una posizione privilegiata che le consentirà di fare la differenza. [*A*]*nche se la responsabilità primaria della sicurezza incombe ai singoli Stati membri, negli ultimi anni è emerso chiaramente che la sicurezza di uno Stato membro è la sicurezza di tutti*. L'UE può apportare una risposta multidisciplinare e integrata (enfasi aggiunta dall'autore)[77].

Sotto altro profilo, la Commissione sottolinea come per ragioni legate alla paura di compromettere la sicurezza nazionale gli attori principali tanto del settore pubblico quanto di quello privato sono stati poco propensi a condividere informazioni di sicurezza[78], ancorché "la massima efficacia la otteniamo quando siamo tutti pronti a sostenerci l'un altro"[79]. Non a caso, una delle ragioni che ha portato alla riforma della direttiva NIS è stata proprio l'insufficiente e non sistematica condivisione di informazioni di cybersicurezza tra Stati membri, e tra operatori di servizi essenziali, con conseguenze negative per l'efficacia delle misure di sicurezza e per il livello di consapevolezza situazionale comune dell'UE[80].

Connesso a ciò, la recente adozione in seno al Consiglio dell'UE del 'Cyber Blueprint'[81] testimonia la presa d'atto degli Stati membri della necessità di rafforzare la rilevanza sovranazionale delle crisi e incidenti su larga scala di cybersicurezza. Infatti, per quanto la responsabilità primaria nella gestione degli incidenti e delle crisi cibernetiche rimanga degli Stati membri, le sfide poste dal cyberspazio, già evidenziate, unitamente alle interdipendenze e connessioni tra istituzioni dell'UE e Stati membri, richiedono una stretta cooperazione tra Stati membri e Unione a livello tecnico, operativo e politico[82]. Il Cyber Blueprint si basa sul quadro dei meccanismi integrati di risposta politica alle crisi (IPCR), che permette all'UE di agire in risposta ad una crisi, a condizione che lo Stato interessato attivi la clausola di solidarietà ex Art. 222 TFUE.

Sul piano dell'azione esterna, poi, l'Unione ha progressivamente inquadrato la

[77] Commissione europea, *Strategia dell'UE per l'Unione della sicurezza,* COM(2020), 605 final, p. 1.
[78] La condivisione di informazioni è un esempio di come i principi di cooperazione e collaborazione possano essere attuati nella cybersicurezza: valorizzando la conoscenza, l'esperienza e le capacità collettive di una determinata comunità di condivisione, i partecipanti a tali accordi aumenterebbero la propria consapevolezza e svilupperebbero una comprensione più completa del panorama delle minacce. Si veda, *ex multis,* NIST Special Publication 800-150*, Guide to Cyber Threat Information Sharing*, 2016.
[79] Commissione europea, *Strategia dell'UE per l'Unione della sicurezza,* cit., p. 7.
[80] Commissione europea, *"Results of ex-post evaluations, stakeholder consultations and impact assessments", accompanying the Commission proposal for a directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148*, COM(2020) 823 final (NIS2 Directive proposal).
[81] Consiglio dell'Unione europea, *Recommendation on an EU blueprint for cyber crisis management*, 9794/25, 6 giugno 2025.
[82] Cons. 3 e 5, Cyber Blueprint.

cybersicurezza all'interno della Politica estera e di sicurezza comune (PESC) sin dalla prima Strategia, ancorché – come nel caso della superficie d'azione legata al funzionamento del mercato interno – sia assente una base giuridica specifica: come giustamente rilevato in dottrina,

> la PESC si configura, oggi, come un laboratorio istituzionale in cui l'Unione sperimenta nuove forme di azione esterna in ambiti tradizionalmente riservati agli Stati membri, estendendo i confini del proprio intervento in materia di sicurezza (digitale) e contribuendo, seppure in via indiretta, al processo di costituzionalizzazione del cyberspazio europeo[83].

Infine, nel quadro della Strategia europea di sicurezza interna "ProtectEU" dell'aprile 2025, la Commissione preannuncia la proposta di una revisione del Cybersecurity Act[84], che rafforza e aggiorna il mandato dell'ENISA, anche attraverso maggiori risorse e nuovi compiti, alla luce dei recenti obblighi aggiunti dalla legislazione UE (in particolare NIS2 e CRA), specificando al contempo che "non sostituirà i CSIRTs nazionali"[85]. Complementare al più ampio pacchetto di riforma previsto dal cd. Digital Omnibus, la Commissione ha anche proposto emendamenti mirati alla direttiva NIS2[86]. In particolare, l'ENISA avrebbe nuove e importanti responsabilità operative nel quadro dell'assistenza reciproca tra Stati membri verso soggetti che forniscono servizi o che dispongono di infrastrutture di rete e sistemi in più giurisdizioni: su richiesta delle autorità nazionali, l'ENISA parteciperebbe alle azioni di supervisione congiunta[87].

Nel contesto specifico della cybersicurezza, queste proposte di riforma hanno avuto una spinta politica dalle Conclusioni del Consiglio dell'UE nel maggio 2024: se da una parte il Consiglio sottolineava l'efficacia del paradigma regolatorio europeo, imperniato sull'approccio della gestione del rischio (*ex ante regulation*), dall'altra chiedeva una sistemazione dei diversi obblighi andati stratificandosi, al fine di evitare frammentazione e sovrapposizioni regolatorie, che determinano costi e incertezza, preservando così i benefici

[83] F. Casolari, F. Ferri, S. Villani, "La costituzionalizzazione della cybersicurezza nell'ordinamento dell'Unione europea", cit., p. 38.
[84] Commissione europea, *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)*, 20 gennaio 2026.
[85] *Ibid.*, p. 6.
[86] Commissione europea, *Proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2]*, 20 gennaio 2026.
[87] Art. 1, punto 12, che introduce un nuovo Art. 37a nella direttiva NIS2.

del mercato unico[88].

4. Lo Stato colpisce ancora: il caso italiano

Già all'inizio degli anni '90, il governo degli Stati Uniti iniziò a classificare rischi, minacce e incidenti cibernetici come minacce alla sicurezza nazionale, in ragione degli obiettivi: centrali elettriche, banche, il controllo del traffico aereo o le forze armate[89]. In altre parole, l'infrastruttura critica del paese[90]. Così, anche in Europa gli Stati iniziano a inquadrare le crescenti minacce cibernetiche in termini di tutela della sicurezza nazionale, attribuendo pertanto responsabilità agli apparati tradizionalmente posti a tutela di quest'ultima dagli ordinamenti nazionali.

La frammentazione del potere politico avviene attraverso la decentralizzazione dell'autorità e delle funzioni di governo verso il basso (localizzazione), verso l'alto (sovranazionalizzazione) o lateralmente (privatizzazione)[91]. Come visto nelle sezioni precedenti, nel caso della *governance* della cybersicurezza in Europa, la frammentazione del potere avviene soprattutto nelle ultime due forme citate. La presente sezione indaga pertanto la reazione degli Stati a queste spinte centrifughe, soprattutto focalizzandosi sulla direttrice della sovranazionalizzazione, mettendo in luce come l'evoluzione della normativa nazionale in materia di cybersicurezza risenta della prassi a ricorrere ampiamente alla facoltà, in forza del diritto primario dell'UE[92], di imporre requisiti di (cyber)sicurezza ulteriori rispetto a quelli già previsti a livello sovranazionale, oppure a limitare una maggiore "europeizzazione" della cybersicurezza.

Sotto il primo profilo, è questa tendenza all'adozione di requisiti nazionali eterogenei,

[88] Consiglio dell'Unione europea, *Council Conclusions on the Future of Cybersecurity: implement and protect together*, 21 maggio 2024, p. 7.
[89] M. Warner, "Cybersecurity: A Pre-history", *Intelligence and National Security,* 27 (2012), 5, pp. 781-799.
[90] Come rilevato in G. Gabrielli, "La governance internazionale della cybersicurezza: cyber attacchi contro infrastrutture critiche nella prospettiva dello *jus ad bellum*", cit., p. 87, a livello internazionale non esiste una chiara e riconosciuta definizione di 'infrastruttura critica', sebbene la risoluzione UNGA del 2003 identifichi diversi settori essenziali degli Stati. A livello europeo, invece, la direttiva (UE) 2022/2557 relativa alla resilienza dei soggetti critici definisce, all'art. 2, punto 4, infrastruttura critica come "un elemento, un impianto, un'attrezzatura, una rete o un sistema o una parte di un elemento, di un impianto, di un'attrezzatura, di una rete o di un sistema, necessari per la fornitura di un servizio essenziale".
[91] M. Dunn Cavelty, F. Egloff, "The Politics of Cybersecurity", cit., p. 42.
[92] Con riferimento non solo al già citato Art. 4, para. 2, TUE, ma anche all'Art. 346, lett. a, TFUE.

specie in ambiti come la gestione degli incidenti e gli obblighi di sicurezza, a far emergere in modo paradigmatico il sopracitato "dualismo disfunzionale", nei termini già colti dal c.d. "Rapporto Letta", laddove si osserva che la frammentazione delle prescrizioni di sicurezza nazionali finisce per erodere i benefici del mercato unico, aumentare i costi e l'incertezza per gli operatori e, soprattutto, ostacolare lo sviluppo di capacità di cyber-resilienza e di sicurezza robuste, impedendo lo sfruttamento di architetture di rete centralizzate e di economie di scala[93]. Per quanto riguarda il secondo aspetto, ciò emerge in modo evidente – come già accennato nella precedente sezione – nell'ambito della condivisione delle informazioni, aspetto cardine di una concezione collettiva di sicurezza[94].

Prendendo in esame, in particolare, il contesto italiano, le prime iniziative legislative in materia di cybersicurezza sono inquadrate nel Sistema di informazione per la sicurezza della Repubblica: nel 2012 viene riconosciuto al Presidente del Consiglio dei ministri il potere di impartire al Dipartimento delle informazioni per la sicurezza (DIS) e alle agenzie di intelligence "direttive per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali"[95].

Tuttavia, è solo con l'istituzione nel 2019 del Perimetro di Sicurezza Nazionale Cibernetica ('PSNC')[96] che l'Italia si dota di un autonomo quadro regolatorio in materia di sicurezza delle reti, dei sistemi informativi e dei servizi informatici, dal momento che fino ad allora questo consisteva nel decreto di recepimento della direttiva NIS[97]. La ratio del PSNC risiede espressamente nella necessità di assicurare un livello elevato di cybersicurezza di reti, sistemi informativi e servizi ICT delle pubbliche amministrazioni, nonché di enti e operatori nazionali pubblici e privati dai quali dipendono "il funzionamento essenziale dello Stato ovvero al prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e *dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la*

[93] E. Letta, *Much more than a market – Speed, Security, Solidarity: Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens*, 2024, p. 59.
[94] F. Serini, "Collective cyber situational awareness in EU. A political project of difficult legal realisation?", cit., p. 10.
[95] Art. 1, comma 3-*bis*, della l. n. 124/2007, introdotto dalla l. n. 133/2012.
[96] D.l. 21 settembre 2019, n. 105.
[97] D.lgs. 65/2018.

sicurezza nazionale (enfasi dell'autore)"[98].

La formulazione del primo articolo del decreto che istituisce il "perimetro" è di carattere programmatico e mostra la volontà del Governo italiano di regolare un'area specifica della sicurezza nazionale; evidentemente, tali interessi giustificano "poteri ampi ed effetti limitativi dell'iniziativa economica e dell'agire privato"[99]. Ad un alto livello di astrazione, il PSNC introduce diversi obblighi di natura preventiva per mitigare *ex ante* il rischio di incidenti da cui possa derivare, appunto, un pregiudizio per la sicurezza nazionale. Sia l'approccio regolatorio (anticipazione della minaccia e gestione del rischio) che il contenuto della maggior parte degli oneri per i soggetti ricompresi ricalcano il quadro europeo della NIS: obblighi di comunicazione[100]; di adozione di misure tecniche ed organizzative di gestione del rischio di cybersicurezza[101]; di allineamento di processi interni, soprattutto con riferimento alla notifica di incidenti[102]. Gli adempimenti legati agli approvvigionamenti e all'affidamento di forniture di beni, sistemi e servizi ICT[103] sono invece requisiti originali del PSNC che non trovano corrispettivo nella normativa europea.

La ratio di queste ultime disposizioni (cioè comunicare, in virtù del collegamento con la tutela della sicurezza nazionale, a organi governativi procedure ed istituti altrimenti lasciati all'iniziativa privata) è condivisa con i c.d. poteri speciali esercitabili dal Governo in diversi settori di rilevanza strategica per la difesa e la sicurezza nazionale, attraverso i quali può dettare specifiche condizioni od opporsi all'acquisto di partecipazioni e porre il veto

[98] Art. 1, comma 1, d.-l. 105/2019.
[99] E. Buoso, "Ritorno al futuro: il perimetro di sicurezza nazionale cibernetica", in P. Heritier, S. Rossa (a cura di), *Cybersecurity e istituzioni democratiche. Un'indagine interdisciplinare: diritto, informatica e organizzazione aziendale*, Mimesis, 2025, p. 38.
[100] Art. 1, comma 2, lett. b: ai soggetti PSNC è imposto di predisporre e aggiornare almeno annualmente un elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza e di trasmetterlo all'ACN. Il DPCM 30 luglio 2020, n. 131 specifica i criteri e le modalità procedurali.
[101] Art. 1, comma 3, lett. b: i soggetti PSNC adottano misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici. Il DPCM 14 aprile 2021, n. 81 individua puntualmente le misure nell'Allegato B e impone tempi di implementazione graduati (categorie A e B).
[102] Art. 1, comma 3, lett. a: i soggetti PSNC notificano all'ACN gli incidenti aventi impatto su reti, sistemi e servizi di pertinenza. Il DPCM 14 aprile 2021, n. 81 tipizza gli incidenti (Allegato A) e stabilisce i termini per la notifica decorrenti dal momento di conoscenza (entro 6 ore per gli incidenti "meno gravi", entro 1 ora per i "più gravi").
[103] Per l'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici 'perimetrati', i soggetti PSNC devono dare comunicazione al Centro di Valutazione e Certificazione Nazionale presso l'ACN. Il DPR 5 febbraio 2021, n. 54 disciplina in dettaglio la "comunicazione di affidamento" (tempi e contenuti minimi, inclusa un'analisi del rischio associata) e il procedimento di verifica e valutazione (verifiche preliminari, preparazione ed esecuzione test, eventuali prescrizioni del CVCN).

all'adozione di determinate delibere societarie[104]. Non a caso, tra i settori interessati dalla normativa *golden power* figurano i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, nonché "ulteriori servizi, beni, rapporti, attività e tecnologie rilevanti ai fini della sicurezza cibernetica"[105].

Se è vero che la direttiva NIS1 non ricomprendeva nell'ambito di applicazione gli enti della pubblica amministrazione, nel 2019 era già iniziato il processo di revisione dello strumento, che culminò con la pubblicazione della proposta di direttiva NIS2 nel 2020[106]. Tra gli aspetti più critici del quadro previgente, su cui interviene la riforma, c'è proprio il ristretto ambito di applicazione dello strumento: la direttiva NIS2 non a caso inserisce il settore della pubblica amministrazione tra quelli ad 'alta criticità' dell'allegato I. Appare quindi lecito domandarsi quale fosse l'opportunità di prevedere norme che, in molti casi, si sarebbero sovrapposte, per la maggior parte dei soggetti, agli oneri derivanti dal riformato quadro NIS[107]. Evidentemente, per evitare duplicazioni, il legislatore ha dovuto prevedere, nella normativa di recepimento della NIS2, un raccordo con la normativa Perimetro[108].

Così, il PSNC si innesta sul medesimo modello europeo *risk-based*[109], ma lo "nazionalizza" con una diversa base giuridica. Ne deriva una manifestazione paradigmatica del dualismo disfunzionale: lo Stato esercita la competenza di sicurezza nazionale per introdurre un regime parallelo per la gran parte degli obblighi e per la maggior parte degli operatori, anche quando il processo di revisione UE rendeva già prevedibile la sovrapposizione. Peraltro, gli obblighi in materia di approvvigionamento e affidamento di forniture accentuano la dimensione di *supply chain security* come leva di sovranità nazionale, al prezzo, però, di una frammentazione del quadro UE, con conseguente erosione dei benefici del mercato interno.

[104] Si veda M. Matassa, "I golden powers italiani nel settore della difesa e sicurezza nazionale", *Il diritto dell'economia*, 113 (2024), 1.
[105] Art. 1-*bis*, d.l. 15 marzo 2012, n. 21, come modificato dall'Art. 28, d.l. 21 marzo 2022, n. 21.
[106] Commissione europea, IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, p. 10.
[107] S. Schmitz-Berndt, P.G. Chiara, "One Step Ahead: Mapping the Italian and German Cybersecurity Laws against the Proposal for a NIS2 Directive", *International Cybersecurity Law Review*, 3 (2022), pp. 307-310; M. Ripiego, "La sicurezza informatica nell'ordinamento italiano: criticità e opportunità a seguito dell'entrata in vigore della direttiva europea NIS2", *Cammino Diritto*, 2 (2022).
[108] Art. 33, d. lgs. 138/2024.
[109] G. De Gregorio, P. Dunn, "The European risk-based approaches: Connecting constitutional dots in the digital age", *Common Market Law Review,* 59 (2022), 2; P.G. Chiara, F. Galli, "Normative Considerations on Impact Assessments in EU Digital Policy", *Medialaws*, 1 (2024).

Tale dinamica di sovrapposizione funzionale, soprattutto, rischia di ottenere l'effetto opposto a quello desiderato (cioè, l'innalzamento della resilienza collettiva), perché trasforma l'integrazione in un mosaico di *compliance*.

Il quadro analitico proposto in questo saggio prova ad inquadrare i motivi per i quali il legislatore nazionale ha perseguito, e tuttora persegue, tale politica. Emblematica in tal senso è la l. 90/2024, che anticipa diverse norme di adeguamento alla direttiva NIS2 per una serie di soggetti rimasti esclusi dall'ambito di applicazione soggettivo del PSNC (es., città metropolitane, ASL, ecc.)[110], all'epoca già entrata in vigore, creando altrimenti evitabili problemi di coordinamento con il quadro di matrice eurounitaria, come evidenziato da diversi commentatori[111]. Per altro verso, poi, il capo II della legge inasprisce la risposta penale mediante disposizioni di natura sostanziale e processuale, mirate al contrasto dei reati informatici. Come già visto (sezione 2.3), numerose sono le sfide che incidono negativamente sull'efficacia di una risposta di stampo *puramente* penalistico. Infine, la legge n. 90/2024 interviene anche nell'ambito del *procurement,* sulla scia della novella dell'art. 108, comma 4 del Codice dei contratti pubblici, che reca disposizioni specifiche in materia di approvvigionamento di beni e servizi digitali, prevedendo che, in tali attività, le stazioni appaltanti ai fini dell'individuazione del miglior rapporto qualità-prezzo per l'aggiudicazione, tengano sempre in considerazione gli elementi di cybersicurezza, attribuendovi specifico e peculiare rilievo nei casi in cui il contesto di impiego sia connesso alla tutela degli interessi nazionali strategici. In particolare, l'art. 14, comma 2, lett. e) prevede criteri di premialità per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane, UE o di paesi terzi – individuati nell'Allegato 3 del DPCM 2 ottobre 2025 – e tra i quali figura anche Israele. Tale previsione non può che sollevare quantomeno perplessità, *inter alia,* sul piano del perseguimento della c.d. sovranità digitale.

Un ultimo indicatore di frizione istituzionale su cui ci soffermeremo è rinvenibile nel decreto di recepimento della direttiva NIS2, in particolare, all'art. 2 dedicato alle definizioni. Il legislatore dà infatti tre definizioni diverse per: i) "sicurezza dei sistemi informativi e di

[110] A titolo esemplificativo, viene inserito un obbligo di notifica degli incidenti con termini perfettamente corrispondenti a quelli della direttiva NIS2 (24 ore per una segnalazione dell'incidente e 72 ore per una notifica completa).

[111] Si vedano i contributi contenuti nel fascicolo monografico *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2*, a cura di G. Fiorinelli e M. Giannelli, in *Rivista Italiana di Informatica e Diritto*, 2024.

rete", concetto antesignano di 'cybersicurezza' a livello europeo, come abbiamo visto; ii) "sicurezza informatica"; e iii) "cybersicurezza". Mentre "sicurezza informatica" si riferisce alla definizione di cybersicurezza contenuta nel reg. Cybersecurity Act, e che dal 2019 in poi costituisce il parametro concettuale per il diritto europeo (tant'è vero che i successivi atti giuridici rinviano a tale regolamento per la definizione di cybersicurezza), "cybersicurezza" identifica invece l'insieme delle "attività […] necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico"[112]. Gli oggetti materiali tutelati dalle citate definizioni sono i medesimi (reti, sistemi informativi e servizi informatici), così come l'obiettivo strumentale (assicurare disponibilità, integrità, riservatezza) e il fattore di rischio (minacce informatiche).

5. Alcune riflessioni conclusive

Tra le molte e diverse sfide del nostro tempo, la cybersicurezza più di tutte, forse, rivela la fragilità e, in un certo qual modo, la crisi del tradizionale paradigma della fornitura della sicurezza da parte dei (soli) soggetti statali. Evidentemente, il concetto di "crisi" non indica qui una perdita della sovranità, ma piuttosto un incremento dello scarto tra titolarità formale dei poteri e capacità effettiva di produrre sicurezza in un dominio transnazionale e tecnicamente opaco, caratterizzato dalla dipendenza strutturale dal settore privato. Modelli di *governance* ibridi, multilivello e policentrici di gestione del rischio, emersi in Europa dapprima sul piano sovranazionale, appaiono come risposte efficaci a questi fallimenti di mercato e al dilemma dell'esercizio della sovranità sullo spazio digitale[113].

Le tre caratteristiche della 'crisi strutturale' individuate in questo lavoro (extraterritorialità delle minacce, difficoltà di attribuzione della responsabilità ed enforcement, dipendenza da infrastrutture e fornitori privati) costituiscono le condizioni che rendono prevedibili due esiti misurabili. In primo luogo, una risposta regolatoria efficace tende a spostarsi verso strumenti che agiscono "a monte" dell'incidente di cybersicurezza (o attacco), imponendo obblighi e

[112] Art. 2, comma 1, lett. s, d.lgs. 138/2024.
[113] P. Timmers, "The European Union's cybersecurity industrial policy", *Journal of Cyber Policy,* 3 (2018), 3.

misure tecniche e organizzative a soggetti pubblici e privati al fine di aumentare il livello di resilienza. Il modello classico di enforcement, di matrice tipicamente penalistica, basato sull'attribuzione della responsabilità, è strutturalmente incerto nel contesto del cyberspazio. In secondo luogo, limitatamente al contesto europeo, una risposta scoordinata ed esclusivamente nazionale, che non promuova un'*effettiva* cooperazione a livello sovranazionale (ad es., attraverso una piena condivisione di informazioni), produce inevitabilmente frammentazione e disallineamenti, poiché il dominio non è territorialmente confinabile.

La traiettoria delineata dalle tre Strategie UE e dagli strumenti che ne hanno tradotto l'impianto in obblighi giuridici mostra come il suesposto paradigma regolatorio tratti la cybersicurezza come rischio sistemico del mercato interno e delle infrastrutture critiche, governabile soprattutto tramite obblighi di gestione del rischio lungo le filiere di approvvigionamento; standardizzazione e certificazione come dispositivi di governo tecnico; misure di gestione delle vulnerabilità; cooperazione amministrativa e scambio informativo; costruzione di capacità operative e di risposta; e, al contempo, tentativi di ri-territorializzazione tramite, ad esempio, requisiti di localizzazione dei dati.

In questo contesto, l'analisi ha provato a mettere in luce ciò che ho definito "dualismo disfunzionale", e le ragioni che ne stanno alla base, rivelando la fragilità del modello del *regulatory security state*[114] a livello nazionale in materia di cybersicurezza nella misura in cui: a) si sovrapponga, ancorché nelle aree di esclusiva competenza (es., sicurezza nazionale), agli *strumenti* adottati a livello sovranazionale; b) rimanga ancorato a tradizionali risposte di sicurezza *ex post*[115], e non invece informate da logiche anticipatorie[116]; c) ostacoli politiche e meccanismi di coordinamento a livello europeo di risposta agli incidenti e gestione delle crisi, soprattutto attraverso lo scambio di informazioni rilevanti per la cybersicurezza.

Pier Giorgio Chiara
Università di Bologna
piergiorgio.chiara2@unibo.it

[114] A. Kruck, M. Weiss, "The regulatory security state in Europe", *Journal of European Public Policy*, 30 (2023), 7.
[115] Le sfide analizzate nella sezione 2 rendono problematico un modello regolatorio fondato su interventi successivi al verificarsi del danno. Cfr. C. Sunstein, *Risk and Reason*, Cambridge University Press, 2002.
[116] R. Brownsword, K. Yeung, *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, Hart Publishing, 2008.