PA Persona e Amministrazione
Ricerche Giuridiche sull'Amministrazione e l'Economia

Manfredi Matassa
Dottorando di ricerca presso il Dipartimento di Giurisprudenza dell'Università di Palermo
manfredi.matassa@unipa.it

Una strategia nazionale a difesa del Cyberspazio

A national strategy for the defense of cyberspace

Sintesi

L'articolo intende proporre un'analisi circa lo stato dell'arte della sicurezza cibernetica in Italia, prestando particolare attenzione alle principali novità contenute all'interno della Strategia Nazionale di Cybersicurezza 2022-2026. Nello specifico, dopo aver offerto un inquadramento giuridico del fenomeno degli attacchi informatici, il contributo intende approfondire con una visione critica le future sfide che vedranno l'Italia e l'Europa protagoniste nella difesa del proprio "dominio cibernetico".

Abstract

The article intends to propose an analysis about the state of the art of cyber security in Italy, paying particular attention to the main innovations contained in the National Cybersecurity Strategy 2022-2026. Specifically, after offering a legal framework of the concept of cyber-attack and the context that has elevated the theme of cybersecurity to an essential element for the exercise of the sovereignty of States, the contribution intends to deepen with a critical vision the future challenges that will see Italy protagonist in the defense of its cyber domain.

Parole chiave: sicurezza cibernetica – Strategia Nazionale di Cybersicurezza – Direttiva NIS – attacchi cibernetici – organizzazione della sicurezza cibernetica

Keywords: cyber-security law – Cyber-security National Strategy – NIS Directive – law of cyber-attacks – organization of cyber-security

1. Premessa

Internet è il più grande spazio pubblico che l'umanità abbia conosciuto, una rete senza alcun sovrano che avvolge l'intero pianeta[1]. La natura libertaria, quasi anarchica, della rete ha indotto le organizzazioni di tutto il mondo a riflettere su modelli di regolazione idonei a perimetrare un territorio privo di confini. Nel 1996, in occasione del tentativo del legislatore americano di imporre una politica restrittiva in materia di controllo delle telecomunicazioni, John Perry Barlow formulò la celebre dichiarazione di indipendenza del Cyberspazio riferendosi ai Governi del mondo come «stanchi giganti di carne e di acciaio» incapaci di comprendere la portata della rivoluzione in corso[2]. A quel tempo il CERN aveva annunciato da appena cinque anni la nascita del *world wide web*[3], la rete internet connetteva tuttalpiù dieci milioni di computer e il termine "Cyberspazio" si riferiva esclusivamente ad un universo alternativo teorizzato in un romanzo fantascientifico[4]. In tale contesto, internet era ancora immaginato come uno spazio virtuale lontano dai problemi geopolitici ed economici del mondo reale e non assoggettabile al controllo di alcun governo[5].

---

1 S. Rodotà, *Il diritto di avere diritti*, Bari, Laterza, 2012, 358.

2 J. P. Barlow, *A declaration of independence of Cyberspace*, 1996, reperibile su https://www.eff.org/it/cyberspace-independence.

3 W3C, *A little history of World Wide Web (from 1945 to 1995)*, 2000, reperibile su https://www.w3.org/history.htlm.

4 Il termine "*cyberspace*" venne coniato nel 1982 da William Gibson per fare riferimento a un luogo immaginario di allucinazioni tecnologiche contrapposto a uno spazio reale ormai al collasso. Sebbene la prima comparsa di questo termina sia da attribuire al racconto "la notte che bruciammo Chrome" (W. Gibson, *Burning Chrome*, *Omni*, vol. 46, 1982, 72 ss.), il termine ha trovato un diffuso utilizzo a seguito della pubblicazione del successivo e più fortunato romanzo "Neuromante" (Id., *Neuromancer*, New York, 1984, 62).

5 Sull'evoluzione del rapporto tra "cyber e sovranità" si rimanda a K.E. Eichensehr *et. al.*, *The cyber-law of nations*, in *Georgetown Law Journal*, 2, 2015, 317 ss. Tale contributo, dopo aver fornito una sommaria descrizione del concetto di cyberspazio, individua tre precise fasi che hanno segnato nel corso del tempo il rapporto tra sovranità e cyberspazio. In una prima fase, agli albori della nascita di internet, la sovranità del dominio cibernetico si riteneva attribuita agli stessi utenti della rete sulla falsariga dei principi espressi nella citata Dichiarazione di indipendenza del Cyberspazio (*Cyber as Sovereign*). La seconda fase di questo rapporto è caratterizzata dallo sviluppo del concetto di "*Internet as a 'Place'*", volto a negare quell'assunto secondo cui la rete fosse un "luogo" separato rispetto al resto del mondo, e la conseguente soggezione di quest'ultima alla sovranità dei singoli Stati in cui opera (*Soverignity over Cyber*). La terza e più moderna elaborazione attribuisce inquadra la sovranità della rete come un problema su scala glo-

Nessuno allora avrebbe immaginato che, da lì a qualche anno, sarebbe stata invece l'inarrestabile espansione del Cyberspazio ad invadere quasi ogni aspetto della vita reale[6].

Oggi l'impegno sul fronte della sicurezza cibernetica deve considerarsi un prerequisito essenziale per garantire la solidità della struttura economica e sociale di uno Stato. La storia recente ha dimostrato come un'organizzazione ostile, che sia un insieme di privati o un altro Stato, possa ricorrere a *cyber-attacks* non solo per sospendere l'erogazione di servizi pubblici essenziali di un intero Paese o comprometterne le infrastrutture di difesa, ma anche per interferire nella formazione dei processi decisionali indispensabili per la vita di una qualsiasi democrazia. A quanto detto occorre aggiungere che l'ingresso dell'Internet of Things (IoT)[7] nella nostra vita quotidiana ha portato con sé indiscutibili vantaggi, ma ha anche coinvolto il cittadino nel «mondo delle tecnologie ad alto rischio»[8] in modo spesso inconsapevole.

Nel corso dell'ultimo ventennio l'argomento della sicurezza informatica è stato oggetto di numerosi studi che hanno coinvolto trasversalmente quasi ogni ambito del sapere, ma solo in anni recenti è emerso il ruolo di grande rilie-

---

bale da affrontare attraverso i tradizionali strumenti di diritto e politica internazionale (*Global Cyber Governance*). Per un ulteriore approfondimento sul tema si vedano, tra gli altri, J. GOLDSMITH, *The internet and the abiding significance of territorial sovereignty*, in *Indiana Journal of Global Legal Studies*, 2, 1998, 475 ss. e J. GOLDSMITH, T. WU, *Who controls the internet? Illusion of a borderless world*, Oxford, 2006.

6 Per una riflessione circa l'impossibilità di distinguere nella società moderna il mondo online da quello offline, o meglio circa la necessità di continuare a imporre una simile distinzione, si rimanda all'eccellente contributo di L. FLORIDI (A cura di), *The onlife manifesto: being human in a hyperconnected era*, Springer, 2009, 1-17.

7 Il concetto di "Internet of Things" (IoT) è stato impiegato per la prima volta nel 1999 dall'ingegnere inglese Kevin Ahston per descrivere un sistema in cui gli oggetti del mondo fisico potessero essere connessi all'internet attraverso dei sensori (V. SINGHANIA, *The Internet of Things: an overview understanding the issues and challenges of a more connected world*, in *Internet Society*, 2015, 7). Gli esempi applicativi di IoT ad oggi sono innumerevoli: basti pensare alle automobili, alle abitazioni dotate di impianti domotici o anche alle *smart cities* (secondo le stime dell'Unione Europea entro il 2024 saranno circa 22,3 miliardi i dispositivi in tutto il mondo connessi all'IoT). Per un maggiore approfondimento sull'argomento si veda H. WEBER, E. STUDER, *Cybersecurity and the Internet of Things: Legal Aspect*, *in Computer Law & Security Review*, 36, 2016, 726 ss.; A. RAYES, S. SALAM, *Internet of Things: from Hype to Reality*, Springer, 2019, 2 ss.

8 Si fa riferimento al concetto di «world of high-risk technologies» elaborato da C. PERROW, *Normal accidents: living with high-risk technologies*, Princeton University Press, 1984, 3.

vo attribuito alla scienza dell'amministrazione per il raggiungimento degli obiettivi prefissati in materia di cybersicurezza. Come si avrà infatti modo di approfondire nei successivi paragrafi, l'esigenza di protezione verso le sempre più crescenti minacce cibernetiche ha condotto l'Unione Europea e i singoli Stati membri a dotarsi di strutture organizzative con caratteristiche inedite, dando così vita ad un'architettura di notevole complessità e in costante mutamento. Con particolare riferimento al contesto italiano, pur riscontrando una tardiva presa di consapevolezza circa l'importanza del tema rispetto ad altri Stati europei, va riscontrato come le nostre istituzioni abbiano elaborato un modello virtuoso (e con alcuni profili di originalità) da ultimo valorizzato dalla pubblicazione della strategia nazionale di cybersicurezza 2022-2026.

Prima di procedere con l'analisi degli argomenti fin qui richiamati, con particolare riferimento al contenuto della Strategia Nazionale (oggetto di interesse principale di questo contributo), si ritiene opportuno fornire un inquadramento giuridico dei concetti preliminari in materia di *cybersecurity* più rilevanti. Del resto, cercare di comprendere un ambiente virtuale attraverso le sole categorie conosciute nel mondo reale sarebbe un compito sicuramente arduo (se non impossibile).

2. Inquadramento giuridico del fenomeno

Nell'aprile del 2007 il governo estone decise spostare una statua simbolo dell'era sovietica dalla piazza centrale di Tallin in un luogo meno rappresentativo della città, scatenando violenti scontri tra la popolazione russofona e le autorità. La risposta a questi eventi segnò uno spartiacque nella storia recente: un gruppo riconducibile alla Russia avviò un *DdoS attack*[9] dalla durata ventidue

9 Per *Distributed Denial of Service attack* (DdoS) si fa riferimento a un attacco distribuito capace di generare una quantità abbastanza grande di traffico di dati verso un determinato server fino al punto di rallentarne il funzionamento o impedirgli di accettare nuove connessioni. Si tratta di un bombardamento informatico di grande intensità, capace di sospendere il funzionamento di un determinato server per tutta la durata dell'attacco. Rimandando lo studio dell'incidenza degli attacchi *ransomware* nel settore pubblico a contributi più approfonditi (L. T. CONNOLLY, D. S. WALL, *The rise of crypto-ransomware in a changing cybercrime landscape: taxonomizing countermeasures*,

giorni che rese impossibile l'erogazione di alcuni servizi pubblici e commerciali essenziali per la vita del paese, fino a deteriorare (e in alcuni casi a distruggere) i server bersagliati.

Pochi anni più tardi, nel gennaio del 2010 il programma nucleare iraniano subì un brusco rallentamento a causa dell'improvviso guasto di parte della strumentazione utilizzata per l'arricchimento di uranio nella principale centrale del Paese. I sistemi di difesa informatici di allora non rilevarono alcuna anomalia e, certe che lo sviluppo di sistemi digitali offline costituisse un valido strumento di difesa, le autorità iraniane non ritennero che l'incidente fosse stato conseguenza delle ingerenze di un soggetto esterno. La causa del malfunzionamento venne scoperta soltanto nei mesi successivi: un malware capace di autopropagarsi (*worm*) dal peso di soli 500 kilobyte, possibilmente introdotto attraverso l'inserimento di una semplice chiavetta USB, che richiese circa 10.000 giorni di lavoro per la sua creazione. Un progetto troppo grande da realizzare per chiunque non fosse uno Stato-nazione.

Con il passare del tempo divennero sempre più frequenti attacchi informatici non più legati a singoli obiettivi militari o strategici, ma elaborati con l'intento di creare danni economici e reputazionali agli Stati attraverso attacchi diffusi e ad ampio spettro. Si pensi, ad esempio, al *malware* noto come *Wanna Cry* che nel 2017 riuscì a infettare in poco tempo più di 200.000 computer in almeno 74 nazioni cifrando le informazioni contenute nei dispositivi attaccati o, ancora, a *Petya* che negli stessi anni riuscì a infliggere danni a imprese europee e statunitensi per una stima di circa dieci miliardi di dollari.

Le implicazioni di questi eventi non furono immediatamente chiare. Se in un primo momento alcuni autorevoli studiosi ricalcarono con fermezza l'idea

---

in *Computer & Security*, 87, 2019), in questa sede preme in ogni caso sottolineare come tale tipologia di attacco si sia dimostrata particolarmente efficace contro le pubbliche amministrazioni. La natura spesso riservata dei dati posseduti da quest'ultime permette infatti di portare a termine attacchi ransomware "a doppia estorsione" con cui, oltre alla somma richiesta per la decifrazione delle informazioni presenti nel dispositivo colpito, l'attaccante richiede un riscatto aggiuntivo minacciando di rendere pubblici i dati ottenuti.

secondo cui la minaccia cibernetica non potesse essere valutata alla stregua di una minaccia militare in senso stretto[10], gli avvenimenti che si verificarono negli anni successivi smentirono quest'idea dimostrando come il cyberspazio fosse ormai asceso alla «quinta dimensione della conflittualità»[11]. Si accede così ad un momento storico in cui la sicurezza interna, il benessere economico e la vita democratica di uno Stato iniziano a dipendere dalla stabilità e la sicurezza del *cyberspazio*[12]. In tale contesto, prima di soffermarsi sull'importante ruolo affidato alla scienza dell'amministrazione nel contrasto alle minacce cibernetiche, si ritiene opportuno mettere a fuoco il concetto di "attacco cibernetico" e le diverse implicazioni che ne scaturiscono sul piano giuridico.

In letteratura si sono registrati diversi tentativi volti ad elaborare una definizione di "attacco informatico" abbastanza flessibile da adeguarsi alla continua evoluzione di tale fenomeno. Rinviando la ricognizione delle varie definizioni proposte a studi più approfonditi[13], in questa sede ci si può limitare a far luce sull'importante distinzione tra attacchi informatici (*cyber-attacks*), guerra cibernetica (*cyber-warfare*) e crimini informatici (*cyber-crimes*). Sul punto va anzitutto chiarito che la ricostruzione maggiormente condivisa inquadra il rapporto tra attacchi informatici e guerra cibernetica in una relazione da genere a specie: entrambi questi fenomeni condividono le medesime due finalità (distruggere o disturbare le operazioni di un network e finalità politiche o di sicurezza nazionale), ma la *cyber-warfare* si contraddistingue per un ulteriore elemento: il verificarsi di effetti equivalenti a quelli causati da un attacco tradizionale. Il crimine informatico, invece, può ritenersi un fenomeno distinto rispetto ai precedenti, in quanto per essere considerato come tale richiede il coinvolgimento dal lato attivo di attori non statali e la commissione di una condotta tassativamente pre-

10 T. Rid, *Cyber war will not take place*, Oxford University Press, Oxford, 2013.
11 La questione è stata di recente trattata da L. Martino, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica & Società*, 1, 2018, 61-76;
12 L. Denardis, *The internet in everything: freedom and security in al world with no off switch*, Yale University Press, 2020, 97.
13 O.A. Hathaway *et. al.*, *The Law of Cyber-Attack*, in *California Law Review*, 4, 2012, 822-832.

vista dalla legge penale attraverso un sistema informatico[14]. Seguendo tale ricostruzione un crimine informatico può essere considerato un cyberattacco soltanto nel caso in cui integri in via mediata o indiretta i presupposti di "scopo" che contraddistinguono tale categoria, mentre appare dubbia la possibile coincidenza con il fenomeno della guerra cibernetica (sarebbe in questo caso più corretto parlare di cyberterrorismo visto il coinvolgimento di attori non statali).

In tale contesto, se i concetti di crimine informatico e guerra cibernetica trovano il loro paradigma giuridico di riferimento rispettivamente nel diritto penale e nel diritto internazionale dei conflitti armati, l'attività di prevenzione e risposta ai cyberattacchi può ormai ritenersi una vera e propria funzione pubblica autonoma e dai caratteri assolutamente inediti. Non solo, nell'ultimo quinquennio il legislatore ha implementato strutture già esistenti dotandole di mezzi quanto più possibili idonei a fronteggiare le nuove sfide, ma – anche in funzione degli obblighi assunti a livello comunitario – ha istituito diverse strutture *ad hoc* (tra cui una nuova agenzia nazionale). Questo percorso ha in poco tempo permesso la costruzione di una complessa architettura che, oltre ad affidare ad operatori privati e cittadini un ruolo determinante nella realizzazione degli obiettivi prefissati, si caratterizza per lo stretto collegamento funzionale con l'infrastruttura comune di difesa disegnata dall'Unione Europea.

3. La disciplina dell'Unione Europea

In premessa, va sottolineato come l'Unione Europea non sia stata tra le prime istituzioni ad acquisire una piena consapevolezza circa la necessità di adottare in tempi rapidi dei modelli regolatori capaci di affrontare al meglio le future sfide di sicurezza cibernetica. Tuttavia, sebbene in netto ritardo rispetto ad altri *competitors* internazionali come gli Stati Uniti[15], negli ultimi anni l'UE è

14 Per un più chiara comprensione sul rapport tra questi tre concetti si rinvia alla rappresentazione grafica suggerita da Y. Li, Q. LUI, *A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments*, in *Energy Reports*, 7, 2021, 833.
15 Gli Stati Uniti hanno inserito la *cybersecurity* tra le priorità del governo federale già nel 1997 (sul punto si rinvia a D.E. BAMBAUER, *Conundrum*, in *Minnesota Law Review*, 2011, 585-591), di-

riuscita a creare un sistema di sicurezza cibernetica all'avanguardia attraverso diversi interventi ben calibrati. A sostegno di quanto detto è possibile segnalare che, tra i primi venti Paesi inseriti nella più recente classifica del *Global Cybersecurity Index* (GCI), ben undici Stati sono membri dell'UE.

Il processo che ha portato alla creazione dell'attuale architettura di difesa europea è stato però tutt'altro che lineare. Prima ancora di progettare le misure necessarie per fronteggiare il sempre più preoccupante fenomeno degli attacchi informatici, il legislatore europeo è stato chiamato a perimetrare il concetto di "*cybersecurity*" in modo da far fronte alle diverse esigenze (e soprattutto le risorse disponibili) degli Stati membri. Non essendo certamente questa la sede per avventurarsi nella impervia strada della ricerca della più appropriata definizione di *cybersecurity*[16], bisogna in ogni caso rappresentare come ancora oggi questo concetto risulti declinato in maniera diversa non solo a seconda dell'area di regolazione interessata, ma anche sulla base dei diversi obiettivi perseguiti dagli Stati membri. Per meglio comprendere la questione basta evidenziare come nelle strategie dei diversi paesi UE si riscontri ad oggi la coesistenza di almeno diciotto definizioni diverse di "*cybersecurity*"[17].

Nel contesto fin qui delineato, le apparentemente irrisolvibili difficoltà sul piano terminologico non hanno potuto che riversarsi nell'ambito regolatorio: l'architettura europea di cybersicurezza per lungo tempo non è stata altro

---

mostrando una chiara consapevolezza dell'importanza che avrebbe assunto il tema nel determinare i futuri equilibri tra Stati. A testimonianza della complessità della materia trattata può evidenziarsi come, sebbene gli Stati Uniti figurino nel più recente GCI come il paese più virtuoso in materia di sicurezza cibernetica con un punteggio di 100/100, in letteratura non manca chi descrive l'infrastruttura di difesa informatica americana «a mess if not an outright disaster» (D.E. BAMBAUER, *Cybersecurity for Idiots*, in *Minnesota Law Riview*, 1, 2021, 172).

16 Sul punto si rimanda all'approfondimento offerto da D. CRAIGEN *et. al.*, *Defining Cybersecurity*, in *Tecnology innovation management review*, 4, 2014, 13-21, il quale dopo aver analizzato le principali definizioni proposte in letteratura ha elaborato la seguente definizione: «*Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign* de jure *from* de facto *property rights*».

17 Per un approfondimento circa le diverse definizioni contenute nelle diverse strategie nazionali si rimanda a G.G. FUSTER, L. JASMONTAITE, *Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights*, in *The international library of ethics, law and tecnology, 21*, 2020, 105-106.

che la somma dei diversi interventi settoriali, spesso eterogenei, dando così vita a un quadro giuridico fortemente frammentato. Ne risulta ancora oggi un sistema oltremodo complesso, che per un efficace funzionamento richiede un'implementazione tanto su un piano orizzontale (ogni settore oggetto di regolazione deve combinarsi con gli altri), quanto su quello verticale (in funzione dell'indispensabile ruolo affidato agli Stati membri per il funzionamento dell'architettura)[18].

Il primo intervento europeo in materia coincide con la pubblicazione della Strategia dell'Unione europea per la cybersicurezza del 2013[19] con cui sono state delineate tre aree iniziali di intervento: a) miglioramento dei sistemi di sicurezza dei sistemi ICT utilizzati dagli erogatori di servizi essenziali e infrastrutture strategiche; b) miglioramento dei sistemi sicurezza delle comunicazioni, con particolare riferimento alla privacy e alla protezione dei dati personale; c) lotta al cybercrimine. L'intento perseguito dalla prima strategia «di fare dell'ambiente online dell'Unione l'ambiente in linea più sicuro al mondo» dimostra grande ambizione e sfida apertamente, forse in modo troppo ottimista, quell'assunto secondo cui nel *cyberspazio* non possa esistere un ambiente sicuro al 100%.

Ciò nondimeno, la sempre più crescente evoluzione della capacità offensiva dei mezzi di attacco informatico mostrò ben presto i limiti della strategia di difesa europea. Gli ingenti danni causati dagli attacchi *ransomware* noti come *WannaCry* e *Petya* del 2017[20] hanno permesso l'avvio di un processo di profondo ripensamento delle politiche in materia di *cybersecurity* volto a riconoscere un sempre più crescente legame tra la sicurezza cibernetica e benessere di cittadini

18 Sul tema si rinvia a R. A. WESSEL, *Towards EU cybersecurity law: regulating a new policy field*, In *Research Handbook on International Law and Cyberspace*, 2015, 405.
19 Commissione Europea, Strategia dell'Unione Europea per la cybersicurezza: un ciberspazio aperto e sicuro, 7 febbraio 2013, reperibile su https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52013JC0001&from=en.
20 Per un'maggiore approfondimento sul tema e per un'analisi di respiro più ampio sull'evoluzione degli attacchi ransomware si rimanda a R. RICHARDSON, M. N. NORTH, *Ransomware: evolution, mitigation and prevention*, in *International Management Review*, 1, 13, 2017.

e imprese operanti nel territorio dell'Unione. Una delle iniziative più virtuose che ha portato all'avvio di tale percorso di rafforzamento va ricondotta alla pubblicazione della seconda strategia europea per la cibersicurezza del 13 settembre 2017[21], con cui si è disegnato un modello comunitario incentrato sul tre concetti chiave: resilienza, deterrenza e difesa. Tra le principali novità, all'interno della menzionata strategia viene manifestato l'intento di riformare l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) istituita nel 2004[22] in modo da creare un centro di coordinamento di *cybersicurezza* europeo con importante ruolo consultivo nell'elaborazione e nell'attuazione delle politiche europee. Tale obiettivo, di centrale importanza per il raggiungimento del necessario grado di resilienza agli attacchi informatici, è stato realizzato con il successivo regolamento UE del 2019 noto come *Cybersecurity Act*[23], il quale ha attribuito all'Agenzia un mandato permanente volto a offrire un supporto alla gestione operativa degli incidenti informatici da parte degli Stati membri. La strategia per la *Cybersicurezza* dell'UE è stata da ultimo aggiornata nel 2020[24] sulla base dei nove principi affermati nella *Paris call for trust and security in Cyberspace* del 2018, un'iniziativa che ha coinvolti 81 Paesi (tra cui tutti gli Stati europei e gli Stati Uniti) unitamente alle principali società e organizza-

21 Commissione Europea, *Resilienza deterrenza e difesa: verso una cibersicurezza forte per l'UE*, 13 settembre 2013 reperibile su https://eur-lex.europa.eu. Sul punto si veda anche la Raccomandazione (UE) 2017/1584 della Commissione del 13 settembre 2017 relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala, reperibile su https://eur-lex.europa.eu.

22 Regolamento (UE) n. 460/2004 del 10 marzo 2004. Sul ruolo svolto dall'ENISA nella strategia di difesa europea fino al successivo intervento del 2019 si veda G. Christou, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, Palgrave Macmillan, 2016; A. Barrinha, H. Carrapico, *The EU as a Coherent (Cyber) Security Actor*?, in *Journal of Common Market Studies*, 2017, 2-6.

23 Il Regolamento (UE) 2019/881 del 17 aprile 2019 (noto come *Cybersecurity Act*) ha inteso rafforzare il sistema europeo di difesa agendo su due versanti. Da un lato, come già ricordato, ha rafforzato i poteri istituzionali dell'Agenzia europea per la *cybersicurezza*; dall'altro ha permesso l'istituzione di un sistema europeo di certificazione della *cybersicurezza* attraverso l'individuazione di parametri minimi di sicurezza informatica per prodotti, servizi e processi ICT (favorendo anche l'acquisto e lo scambio di dispositivi e sistemi tecnologici in Europa).

24 Commissione Europea, *Strategia dell'UE in materia di cibersicurezza per il decennio digitale*, 16 dicembre 2020, reperibile su https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020JC0018&from=IT.

zioni internazionali operanti nel settore tecnologico e della sicurezza informatica[25]. La principale novità introdotta dalla più recente strategia riguarda l'istituzione di un'unità congiunta per il ciberspazio (nota come *Joint Cyber Unit* o *JCU*) come piattaforma virtuale e fisica per la cooperazione tra le varie comunità di cibersicurezza all'interno dell'UE, ciò «con particolare attenzione al coordinamento tecnico e operativo volto a contrastare gravi minacce e incidenti informatici di natura transfrontaliera».

I menzionati documenti strategici si dimostrano di notevole importanza per il funzionamento operativo del sistema di difesa comune, ma il cuore pulsante del quadro normativo europeo in materia di sicurezza cibernetica va ricercato – oltre che nel già menzionato *Cybersecurity Act* – all'interno della Direttiva 2016/1158[26] (nota come "Direttiva NIS") nonché nella recentissima Direttiva NIS II che ha da poco superato il vaglio delle istituzioni europee.

La Direttiva NIS rappresenta la prima disciplina UE introdotta con l'intento di innalzare la protezione della rete e dei sistemi informativi degli Stati membri dell'Unione attraverso un approccio orizzontale[27].

Il principale merito della richiamata direttiva è stato quello di elaborare dei criteri di identificazione comuni degli operatori di servizi essenziali europeo, affidando agli Stati membri l'onere di trasmettere e aggiornare con cadenza biennale l'elenco dei soggetti pubblici e privati ricavato sulla base dei parametri indicati dall'art. 5 della Direttiva[28] e dei settori indicati dall'Allegato II[29].

---

25 Per un approfondimento sui principi posti alla base della *Paris Call* dell'11 dicembre 2018 si rimanda a https://pariscall.international/en/principles.

26 Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio recante misure per un livello comune di sicurezza delle reti e dei sistemi informativi nell'Unione.

27 Un adeguato approfondimento sul contenuto della Direttiva NIS è offerto da D. Markopoulou *et al.*, *The new EU cybersecurity framework: the NIS Directive, ENISA's role and the Genaral Data Protection Regulation*, in *Computer Law and Security Review*, vol. 35, 2019, 1-11.

28Ai sensi dell'art. 5, par. 2, della Direttiva NIS gli stati membri possono identificare gli operatori essenziali sulla base dei seguenti parametri: «a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociale e/o economiche fondamentali; b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; b) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio».

29 L'Allegato II della Direttiva NIS ha individuato sette macrosettori in cui raggruppare gli operatori di servizi essenziali, più precisamente: energia, trasporti, servizi bancari, servizi finan-

Pertanto, ai fini della NIS non sono ricompresi tutti gli operatori di servizi essenziali intesi in senso ampio, ma soltanto quelli considerati come tali dagli Paesi membri all'esito del procedimento di categorizzazione fissato a monte dal legislatore euro-unionale (prevenendo in ogni caso la possibilità per gli Stati di includere nei settori oggetto di tutela anche soggetti non contemplati dai parametri europei).

Pur dovendo riconoscere alla Direttiva NIS il merito di aver introdotto un nucleo minimo e indispensabile di tutela volto a garantire la continuità dei servizi essenziali a livello europeo, non può ignorarsi come la sempre più crescente evoluzione delle minacce cibernetiche abbia dimostrato alcuni limiti strutturali della disciplina europea. Osservando i parametri per l'individuazione dei soggetti che il legislatore comunitario ha inteso tutelare non può infatti ignorarsi l'assenza di alcuni settori di importanza vitale per la vita e la sicurezza dei cittadini europei: basti pensare che operatori pubblici e privati operanti nel settore della Pubblica Amministrazione, dell'ambiente, del settore alimentare, chimico e nucleare non sono presenti tra i settori indicati nell'Allegato II alla Direttiva. Se è vero che alcuni Stati virtuosi (tra cui come vedremo figura anche l'Italia) hanno provveduto in fase di attuazione della NIS ad ampliare il novero dei soggetti coinvolti, il sistema introdotto nel 2016 non sembra in grado di raggiungere gli obiettivi di armonizzazione prefissati per la costruzione di una "fortezza cibernetica europea".

Il legislatore europeo si è dimostrato consapevole dei limiti fin qui descritti e durante la fase di attuazione della NIS ha lavorato sull'elaborazione di un'ulteriore direttiva (nota come Direttiva NIS II) per colmare le precedenti lacune. Il nuovo testo, approvato dal Parlamento Europeo e dal Consiglio lo scorso novembre ed entrato in vigore il 17 gennaio 2023[30], mantiene intatto lo

ziari e di mercato, sanità, catena di produzione e di distribuzione dell'acqua e infrastrutture digitali.

30 Il testo è reperibile su https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823.

stesso spirito della precedente direttiva ma innalza significativamente il livello di sicurezza delle reti europee partendo proprio dall'assegnazione di nuovi criteri di individuazione dei soggetti da tutelare. La direttiva NIS II ha inteso affrontare le criticità descritte muovendosi in una duplice direzione: da un lato ha esteso gli obblighi di sicurezza a una ricca platea di operatori di servizi essenziali pubblici e privati dapprima non ricompresi nel perimetro applicativo della NIS (*ex multis*, i soggetti pubblici e privati operanti nei settori della produzione di dispositivi medici, dell'ingegneria aerospaziale della gestione dei rifiuti, della produzione e distribuzione di alimenti, dei servizi postali, ma anche tutta la Pubblica Amministrazione); dall'altro ha sottratto ai singoli Stati il compito di identificare gli operatori di servizi essenziali soggetti alla Direttiva attraverso la formulazione di criteri auto-applicativi maggiormente precisi e uniformi.

In conclusione, la direttiva NIS II sembra destinata a cambiare in modo profondo la realtà europea, ma – come già accennato – l'Italia potrà procedere con l'attuazione della nuova Direttiva consapevole di aver già costruito un'infrastruttura di sicurezza cibernetica già in larga parte conforme agli *standard* di tutela richiesti dal legislatore comunitario.

4. L'approccio italiano al tema della sicurezza cibernetica

Nel quadriennio 2018/2021 sono stati registrati a livello mondiale 7144 attacchi informatici, di cui circa 900 hanno colpito l'Europa e ben 185 hanno avuto come target Pubbliche Amministrazioni e società italiane. I dati del rapporto Clusit 2021 fotografano come in Italia il tema della *cybersecurity* sia una minaccia reale e in continua crescita: nel solo 2021 l'Italia ha intercettato 36 milioni di *malware*, circa tre volte in più rispetto all'anno precedente, divenendo così il primo paese in Europa più colpito. A partire dal primo semestre 2022 si è alzato ulteriormente il livello di allerta delle istituzioni italiane a seguito dei numerosi *DdoS Attacks* portati a termine da gruppi organizzati verso numerosi obiettivi – Senato, Ministero della Difesa, Istituto Superiore della Sanità e Poli-

zia di Stato – che hanno determinato un aumento del 350% degli attacchi subiti rispetto all'anno precedente. Oltre a crescere in quantità, ed è questo il dato che desta maggiori preoccupazioni, negli ultimi anni si è peraltro registrato un significativo aumento della capacità degli attaccanti di causare danni significativi al bersaglio (*severity*)[31].

La circostanza per cui le organizzazioni italiane risultino in media maggiormente colpite da attacchi cibernetici rispetto ad altre non può tuttavia ritenersi riconducibile all'inerzia delle istituzioni rispetto a un tema così sensibile. Sebbene in netto ritardo rispetto ad alcuni partner europei[32], negli ultimi anni l'Italia ha elaborato un valido sistema di difesa contro le minacce cibernetiche frutto di scelte politico-legislative sicuramente felici. Comprendendo le implicazioni della velocità e della vastità del cambiamento tecnologico, a partire dal 2013 (DPCM 23 gennaio 2013) le istituzioni italiane hanno adottati una serie di provvedimenti diretti ad acquisire, sviluppare e rafforzare le necessarie capacità per far fronte alle sfide *cyber* del nuovo millennio. Tra questi è possibile ricordare senza alcuna pretesa di esaustività: il d. lgs. 18 maggio 2018, n. 65 (decreto NIS) con cui sono stati introdotti degli obblighi di notifica degli incidente aventi un impatto rilevante sull'erogazione dei servizi ai cittadini; il d.l. 21 set-

31 Nell'ambito della sicurezza informatica per *severity* si fa riferimento alla valutazione della gravità degli impatti generati dagli attacchi secondo una scala progressiva: bassa, media, alta o critica. Nel 2021 gli attacchi a infrastrutture italiane considerate di livello critico equivalgono il 32% del totale, mentre quelli di livello alto si sono verificati nel 47% dei casi. La percentuale complessiva degli attacchi considerati ad elevato impatto è stata dunque vicina all'80% (a fronte del 56% dell'anno precedente).

32 Ad esempio, Francia e Germania hanno elaborato già da diversi anni delle strutture consolidate di difesa dalle minacce cibernetiche che hanno costituito un esempio per gli altri paesi dell'Eurozona: la Francia ha creato un'agenzia destinata alla sicurezza cibernetica (*Agence Nationale de la Sécurité des Systèmes d'Information* - ANSSI) già nel 2008, con la presentazione del Libro Bianco sulla difesa e la sicurezza nazionale durante la presidenza di Nicolas Sarkozy; la Germania, invece, ha fondato nel 1991 – ancor prima della stessa diffusione commerciale di internet – il *Bundesamt für Sicherheit in der Informationstechnik* come autorità dedicata all'ufficio federale della sicurezza informatica. Tra gli Stati europei più virtuosi in materia di *cybersecurity* è necessario inoltre citare Estonia e Lituania che, come già accennato, hanno da tempo costruito un sistema di protezione delle infrastrutture critiche (CIP) di eccellenza in risposta ai gravi e numerosi attacchi subiti nell'ultimo ventennio. Per uno studio dell'architettura di difesa cibernetica francese e tedesca si vedano P. BAUMARD, *Cybersecurity in France*, Springer, 2017 e M. SCHALLBRUCH, I. SKIERKA, *Cybersecurity in Germany*, Springer, 2018.

tembre 2019, n. 105 (decreto Perimetro) istituivo dell'ormai noto perimetro di sicurezza nazionale cibernetica[33]; la strategia Cloud Italia contenuta nel Piano triennale per l'informatica con cui si è incentivata la diffusione di soluzioni basate sul *cloud computing*[34] nel circuito delle Pubbliche Amministrazioni e il recente d.l. 14 giugno 2021, n. 82 istitutivo dell'Agenzia per la Cybersicurezza Nazionale (ACN).

L'efficacia dell'attuale infrastruttura nazionale di *cybersicurezza* è stata di recente messa al vaglio dal *Global Cybersecurity Index*, uno degli strumenti più affidabili per valutare la sicurezza informatica degli Stati. Se da un lato l'ultima rilevazione del 2020[35] ha riconosciuto all'Italia il merito di aver elaborato in breve tempo un sistema di difesa dotato di diversi punti di forza, tra cui l'elevata

33 Attraverso l'istituzione del perimetro nazionale di sicurezza la l. 105/2019 ha inteso assicurare un livello elevato di sicurezza delle reti, dei sistemi e dei servizi informatici utilizzati da quei soggetti, pubblici e privati, che esercitano una «funzione essenziale dello Stato» o che prestano «un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato» anche se al di fuori dall'ambito applicativo delineato dalla Direttiva NIS. La legge 105/1019 ha demandato l'individuazione dei soggetti inclusi e la concreta attuazione del perimetro a successivi decreti del Presidente del Consiglio dei ministri: il DPCM 30 luglio 2020, n. 131 ha definito i criteri di individuazione dei soggetti pubblici e privati nonché le modalità per la predisposizione e l'aggiornamento delle reti, dei sistemi e dei servizi ICT; il DPCM 14 aprile 2021, n. 81 ha definito le procedure e le modalità per la notifica degli incidenti aventi impatto su reti, sistemi e servizi ICT al CSIRT Italia, classificando in categorie – dal meno grave al più grave – gli incidenti aventi impatto sui servizi ICT; il DPCM 15 giugno 2021 ha individuato le categorie di beni, sistemi e servizi ICT che sono tenuti per la cui fornitura è necessario seguire la procedura di valutazione spettante al CVCN; infine, il DPCM 18 maggio 2022, n. 92 ha istituito un sistema di accreditamento e di raccordo degli istituendi laboratori accreditati di prova (LAP). Tra i principali contributi volti ad analizzare il funzionamento del perimetro di nazionale cibernetica si rimanda a B. Carotti, *Sicurezza cibernetica e Stato Nazione*, in *Giorn. dir. amm.*, 5, 2020, 629 ss; S. Miele, *Il perimetro di sicurezza nazionale cibernetica e il nuovo "golden power"*, in G. Cassano, S. Previti (a cura di), *Il diritto di internet nell'era digitale*, Milano, 2020, 186 ss.

34 Per *cloud computing* si intende il paradigma di utilizzo e gestione di risorse computazionali e di servizi informatici erogati su richiesta che possono essere di tre differenti tipologie: servizi sistemistici infrastrutturali (c.d. *Infrastructure-as-a-Service o IaaS);* servizi di piattaforme computazionali per l'erogazione di ambienti di ambienti pre-configurati e amministrati per lo sviluppo di specifiche applicazioni (c.d. *Platform-as-a-Service o PaaS*) o servizi applicativi per l'erogazione di un'applicazione agli utenti finali (c.d. *Software-as-a-Service o SaaS*). La necessità di archiviare i dati detenuti dalle pubbliche amministrazioni in *data center* affidabili e con elevati standard di sicurezza è stata da ultimo sottolineata dal PNNR (principio del "*cloud first*"), il quale ha previsto nell'investimento 1.2 un miliardo di euro per il supporto alla migrazione dei dati delle amministrazioni in servizi cloud qualificati. Per un panorama generale sul tema si segnala C. Millard, *Cloud computing law*, *Oxford*, *OUP Oxford*, 2017; G. Noto La Diega, *Il* cloud computing. *Alla ricerca del diritto perduto nel web 3.0*, in *Europa dir. priv.*, 2, 2014, *577*-658.

qualità degli interventi normativi e delle misure organizzative, dall'altro ha messo in luce la carenza di adeguati mezzi tecnici per affrontare le minacce cibernetiche. In particolare, le principali criticità riscontrate nell'infrastruttura di difesa cibernetica italiana non sembrano discendere esclusivamente dall'arretratezza di investimenti complessivi nel settore[36], ma possono essere ricondotte alla frammentazione e al divario di mezzi e risorse che connota il tessuto produttivo italiano. Se è infatti vero che negli ultimi anni le grandi imprese e le amministrazioni centrali hanno acquisito una sempre maggiore consapevolezza circa l'importanza di dotarsi di adeguati strumenti di tutela avverso le minacce cibernetiche, le piccole e medie imprese appaiono ancora decisamente lontane dal conseguire traguardi significativi a causa dell'indisponibilità dei mezzi finanziari e tecnici necessari per rispondere in modo immediato alle esigenze in materia di *cybersecurity*[37]. Ciò non si limita a creare un problema significativo in termini di sicurezza delle piccole realtà che costituiscono ancora una parte consistente del tessuto produttivo nazionale[38], ma si ripercuote direttamente nelle

35 Il più recente report del 2020 ha assegnato all'Italia un punteggio di 96.13/100, collocandola al ventesimo posto globale e ottavo europeo, individuando come punto di forza dell'architettura nazionale l'indice relativo alle misure organizzative (20/20) e come punto di maggiore debolezza quello relativo alla predisposizione di misure tecniche di difesa (17.56/20). Per un maggiore approfondimento sui dati citati e per un confronto con gli altri paesi si rimanda al contenuto del *Global Cybersecurity Index* 2020 dell'ITU reperibile su https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

36 Sebbene il mercato della *cybersecurity* in Italia ammonti a circa 1,55 miliardi di euro, il rapporto tra spesa in sicurezza e Pil è stato limitato (0,08%). Non solo l'Italia figura infatti ad oggi all'ultimo posto tra i paesi del G7 per investimenti in materia di prevenzione contro le minacce cibernetiche, ma – considerato che la percentuale in paesi con Pil più elevato rispetto al nostro (Francia, Germania e UK) è da due a tre volte più elevata – in valore assoluto la spesa in *cybersecurity* dei paesi del G7 è molto più alta della nostra.

37 Come evidenziato da R. Brighi, P.G. Chiara, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, cit., 30, le imprese non coinvolte nel perimetro nazionale di sicurezza cibernetica sono in genere reticenti a segnalare le vulnerabilità informatiche o gli attacchi subiti per evitare ricadute in termini reputazionali o di co-responsabilità all'evento.

38 La questione è stata approfondita in un report dell'Osservatorio Attacchi Digitali in Italia (OAD), il quale – utilizzando i dati forniti dall'ISTAT – ha evidenziato come il 79% delle impresi italiane siano senza (64,03%) o con solo un dipendente (14,97).

supply chain provocando dei danni particolarmente ingenti anche alle grandi imprese italiane ed europee[39].

In tale contesto, la recente Strategia Nazionale per la Cybersicurezza[40] ha previsto 82 misure da realizzare entro il 2026 con l'obiettivo di instaurare una maggiore collaborazione pubblico-privati secondo un approccio «whole of society». Ciò nondimeno, prima di analizzare i diversi obiettivi individuati dalla strategia e le risorse individuate per far fronte a tale ambiziosa sfida, ragioni di completezza della trattazione suggeriscono di soffermarsi sui diversi attori coinvolti nell'architettura nazionale disegnata dalla strategia italiana di *cybersicurezza*.

5. (segue): Alcuni cenni sull'architettura nazionale di cybersicurezza

Le novità introdotte attraverso il d.l. 14 giugno 2021, n. 82 hanno permesso un profondo ripensamento dell'assetto istituzionale degli attori coinvolti nella materia della *cybersicurezza*[41]. Prima di questo intervento l'ecosistema di difesa cibernetica era articolato sulla base di un'infrastruttura su tre livelli[42] so-

39 Un recente studio condotto nel Regno Unito da Webroot ha messo in evidenza che il 70% degli attacchi informatici a piccole e medie imprese è stato effettuato avendo come obiettivo imprese di grandi dimensioni di cui fossero fornitori. Poiché la realtà italiana non appare dissimile a quella del Regno Unito, se non per il fatto che le dimensioni delle PMI sono ulteriormente ridotte, in assenza di precisi studi in ambito nazionale non sarebbe comunque illogico ritenere che le risorse dedicate siano in Italia ancora inferiori rispetto a quelle in UK.

40 L'art. 2, lett. b), d.l. 14 giugno 2021, n. 82 ha affidato al Presidente del Consiglio dei ministri in via esclusiva il compito di adottare «la strategia Nazionale per la Cybersicurezza sentito il Comitato interministeriale per la cybersicurezza». Attraverso la pubblicazione della strategia nel maggio del 20220 è stata così data concreta attuazione all'obbligo di adozione di una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi imposto dall'art. 7 della Direttiva 2016/1148 (Direttiva NIS). Tra i principali punti individuati dal legislatore europeo come contenuto necessario di tali documenti è possibile ricordare: a) l'individuazione degli obiettivi e le priorità della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi; b) la costruzione di un quadro di governance; c) l'individuazione delle forme di collaborazione tra settore pubblico e settore privato; d) l'indicazione di piani di ricerca e sviluppo; e) un elenco dei vari attori coinvolti in materia di sicurezza delle reti e dei sistemi informativi.

41 Per una trattazione più approfondita sull'infrastruttura nazionale di cybersicurezza disegnata dal d.l. 82/2021 si rimanda all'attenta analisi di F. SERINI, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in *Federalismi.it*, 12, 2022, 244 ss.

42 Sulla base della costruzione del DPCM n. 66 del 19 marzo 2013 (decreto Monti) e la successiva implementazione introdotta con DPCM n. 85 del 17 febbraio 2017 (decreto Gentiloni).

vrapponibile a quella prevista dal «sistema di informazione per la sicurezza della Repubblica»[43]: il primo livello intervento vedeva come protagonista il Presidente del Consiglio dei ministri, al quale era stato assegnato il compito di emanare atti di indirizzo e di predisporre il quadro strategico nazionale e il piano nazionale per la protezione cibernetica e la sicurezza informatica[44]; il secondo livello era stato attribuito a una pluralità di soggetti chiamati ad attuare le direttive politiche, tra questi è stato attribuito un ruolo di maggiore rilievo al Comitato interministeriale per la sicurezza della Repubblica (CISR)[45] e al Nucleo per la sicurezza cibernetica (NSC)[46] istituiti presso la Presidenza del Consiglio e al Dipartimento delle informazioni per la sicurezza della Repubblica (DIS); mentre il terzo ed ultimo era formato dagli organismi di informazione per la sicurezza, chiamati a condurre attività di ricerca, analisi, valutazione e previsione sulle minacce informatiche[47].

L'assetto fin qui descritto con il trascorrere nel tempo ha dimostrato alcuni evidenti limiti, su tutti il suo difficile adeguamento rispetto alla rapida evoluzione delle strategie di attacco e il mancato coordinamento tra i diversi attori coinvolti nell'architettura multilivello nella gestione delle situazioni di crisi. Così, anche in considerazione dell'esponenziale aumento di attacchi informatici

---

43 Si fa riferimento al sistema di difesa delineato dalla l. 3 agosto 2007, n. 124, il quale all'art. 1, lett. a), ha attribuito in via esclusiva al Presidente del Consiglio dei ministri «l'alta direzione e la responsabilità generale della politica dell'informazione per la sicurezza, nell'interesse e per la difesa della repubblica e delle istituzione democratiche posta dalla Costituzione a suo fondamento». Sull'argomento di veda M. FRANCHINI, *Il sistema nazionale delle informazioni per la sicurezza e l'autorità delegata*, in *Giorn. dir. amm.*, 4, 2010, 431 ss., mentre per un approfondimento sul ruolo del Presidente del consiglio nell'architettura nazionale si rimanda B. CAROTTI, *Sicurezza cibernetica e Stato Nazione*, cit., 629 ss.

44 Art. 3, lett. a) e b), del già citato DPCM n. 66 del 19 marzo 2013.

45 Si tratta di un comitato presieduto dal Presidente del Consiglio e composto dall'Autorità delegata, dal ministro degli affari esteri, dal Ministro dell'interno, dal Ministro della difesa, dal Ministro dell'economia e delle finanze e dal Ministro dello sviluppo economico regolato dall'art. 5, comma 3, l. n. 124/127 e dall'art. 4, comma 1, DPCM n. 66/2013.

46 IL NSC è un x interno istituito presso l'Ufficio del Consigliere Militare presso la Presidenza del Consiglio dei ministri a cui gli artt. 8 e 9 del DPCM n. 66/2013 hanno affidato la funzione di supporto al Presidente in materia di sicurezza del "cyberspazio" per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento.

47 Sul punto cfr. art. 7, D.P.C.M. n. 77/2014.

verso il nostro paese, le esigenze di riforma del sistema di difesa nazionale sono divenute nel corso degli anni sempre più pressanti.

In tale contesto, i più recenti interventi hanno portato all'introduzione di nuovi attori pubblici specializzati in materia di cybersicurezza con l'intento di costruire un modello organizzativo autonomo e (parzialmente) distaccato dal sistema di informazione per la sicurezza della Repubblica[48]. Ad eccezione del ruolo assegnato dal d.l. 82/2021 al Presidente del Consiglio dei ministri (il quale mantiene in soluzione di continuità «l'alta direzione e la responsabilità generale delle politiche di cybersicurezza»[49]) il sistema nazionale di sicurezza cibernetica è stato profondamente mutato in conseguenza dell'istituzione di una speciale agenzia incaricata alla «tutela degli interessi nazionali nel campo della *cybersicurezza*[50].

Tale intervento si è reso provvidenziale per semplificare un sistema di competenze a livello nazionale attraverso la costruzione di un unico centro di coordinamento di un'area di intervento trasversale e coinvolgente diversi portatori di interessi. Si è così messo a sistema il sistema organizzativo già esistente attraverso l'introduzione di un importante ruolo di coordinamento che non coinvolge esclusivamente il piano interno, ma anche quello europeo dal mo-

48 Oltre alla già citata Agenzia per la Cybersicurezza nazionale istituita con d.l. 82/2021 – che sarà oggetto di un'autonoma analisi – va anche evidenziato il ruolo attribuito al Comitato Interministeriale per la Cybersicurezza (CIC), il quale si sostituisce al CISR nelle funzioni attribuite dal d. lgs. 18 maggio 2018, n. 65 fatta eccezione per le condizioni di «rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi e servizi» (art. 5, d.l. 21 settembre 2019, n. 105). Quest'ultimo, ai sensi dell'art. 4, comma 2, d.l. 105/2019: «a) propone al Presidente del Consiglio dei ministri gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza nazionale; b) esercita l'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza; c) 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, nonché per la condivisione delle informazioni e per l'adozione di migliori pratiche e di misure rivolte all'obiettivo della cybersicurezza e allo sviluppo industriale, tecnologico e scientifico in materia di cybersicurezza; d) esprime il parere sul bilancio preventivo e sul bilancio consuntivo dell'Agenzia per la cybersicurezza nazionale».
49 Art. 2, comma 1, lett. a), d.l. 14 giugno 2021, n. 82, convertito con modificazioni dalla l. 4 agosto 2021, n. 109.
50 Per una più attenta disamina sulla struttura, sulle funzioni e sull'autonomia dell'Agenzia per la Cybersicurezza Nazionale si rimanda a F. SERINI, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, cit., 248 ss.

mento che l'Agenzia per la cybersicurezza figura quale autorità nazionale competente NIS e "punto di contatto unico" transfrontaliero (PoC NIS)[51].

Presso l'Agenzia sono state inoltre costituite in via permanente diverse strutture costituite da esperti in materie specialistiche. Tra queste occorre ricordare il *Computer security incident response team* (CSIRT Italia), istituito in sede di recepimento della direttiva NIS per garantire la prevenzione, il monitoraggio, l'analisi e la risposta ad incidenti cibernetici e successivamente incardinato presso l'Agenzia[52]; il Centro di Valutazione e Certificazione Nazionale (CVCN) che si occuperà di verificare la sicurezza e l'assenza di vulnerabilità in sistemi ICT in uso nelle infrastrutture da cui dipendono le funzioni e i servizi essenziali del Paese[53] e il riformato Nucleo per la Sicurezza Cibernetica (NSC), adesso incluso all'interno dell'Agenzia ma rimasto a supporto del Presidente del Consiglio dei ministri «per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione di procedure di allertamento»[54].

Il disegno complessivo della nuova architettura vede operare le strutture specialistiche richiamate in sinergia con altre amministrazioni tradizionali a cui sono assegnate prerogative esclusive riconnesse al loro mandato istituzionale. In tale contesto, il comparto intelligence (e in particolare il DIS) è chiamato a fornire all'ACN un quadro informativo utile a orientare progressivamente il

---

51 Ai sensi dell'art. 7, comma 4, del d. lgs. 18 maggio 2018, n. 65 «il punto di contatto unico svolge una funzione di collegamento per garantire la cooperazione transfrontaliera dell'autorità nazionale competente NIS con le autorità competenti degli altri Stati membri, nonchè con il gruppo di cooperazione di cui all'articolo 10 e la rete di CSIRT […]»

52 Il CSIRT Italia è un'unità organizzativa deputata a coordinare la risposta a incidenti informatici, a mitigarne gli effetti e a prevenire il verificarsi di ulteriori eventi ricompresa nel CSIRT network, ossia una struttura di gestione reattiva e proattiva degli incidenti di sicurezza istituita dalla Direttiva NIS (art. 12) con l'obiettivo di promuovere un modello cooperativo tra gli Stati membri dell'UE sotto il coordinamento dell'ENISA. Sulle funzioni del CSIRT Italia, oltre al già citato art. 4, DPCM 8 agosto 2019, si rimanda all'art. 7, comma 3, d.l. n. 82/2021.

53 Il Centro di Valutazione e Certificazione Nazionale (CVCN) è stato originariamente istituito presso il Minestro dello sviluppo economico dall'art. 1, comma 6, del d.l. 21 settembre 2019, n. 105 con l'intento di valutare la sicurezza di bene, sistemi e servizi ICT destinati a essere impiegati nel contesto del Perimetro secondo le categorie previste dal già citato DPCM 15 giugno 2021.

54 Cfr. art. 8, d.l. 14 giugno 2021, n. 82.

potenziamento delle misure volte a garantire la corretta implementazione del piano; il Ministero dell'interno svolge l'attività di prevenzione e contrasto ai crimini informatici in qualità di autorità nazionale di pubblica sicurezza e, infine, il Ministero della difesa svolge funzioni di coordinamento della politica militare, *governance* e capacità militari nell'ambiente cibernetico. A completare il quadro istituzionale fin qui delineato va ricordato il non secondario ruolo affidato alle autorità di settore NIS, ossia quei soggetti pubblici chiamati a individuare nel proprio settore di competenza gli operatori di servizi essenziali da ricomprendere nel perimetro di protezione tracciato dall'Unione[55].

6. (segue): La strategia nazionale di Cybersicurezza

L'adozione della strategia nazionale di cybersicurezza 2022-2026 ha rappresentato uno dei passaggi fondamentali necessari per lo sviluppo coerente e sinergico dell'Agenzia e degli altri attori chiamati ad affrontare le sempre più complesse sfide imposte dalla Cybersicurezza. Nel perseguire tale scopo, il documento programmatico ha affrontato alcune questioni preliminari di centrale importanza in materia di sicurezza cibernetica, partendo dall'individuazione dei rischi e la conseguente definizione delle sfide che il comparto della cybersicurezza sarà chiamato ad affrontare nel prossimo quinquennio.

Con riferimento al primo profilo, la strategia ha individuato tre principali rischi sistemici da scongiurare per la riuscita del sistema di difesa nazionale in materia di cybersicurezza: 1) attacchi cyber volti a sottrarre dati o arrecare danni all'erogazione di servizi del Paese, al suo PIL e alla sua reputazione; 2) utilizzo di riserve e tecnologie sviluppate e prodotti da realtà influenzate (se non controllate) da Governi esteri che potrebbero danneggiare l'infrastruttura di difesa sia in termini di scarsa reperibilità, sia in termini di affidabilità; 3) diffusio-

55 Ai sensi dell'art. 15, comma 1, lett. g), d.l. 82/2021 sono considerate autorità settoriali NIS: il Ministero dello sviluppo economico, il Ministero delle Infrastrutture e della mobilità sostenibile, il Ministero dell'economia delle finanze, il Ministero della salute, il Ministero della transizione ecologica per il settore energia e il Ministero della Transizione Ecologica.

ne nello spazio cibernetico di *fake news*, *deep fake* e campagne di disinformazione volte a polarizzare le opinioni dei cittadini attraverso spazi informativi influenzate da Governi esteri. Con riferimento al secondo profilo, la strategia individua le cinque sfide ritenute fondamentali del prossimo quinquennio: 1) una transizione digitale cyber resiliente della pubblica amministrazione e delle imprese; 2) un'autonomia strategica nazionale ed europea nel settore digitale; 3) la costruzione di un sistema capace di anticipare l'evoluzione della minaccia cyber; 4) il miglioramento della gestione delle crisi cibernetiche; 5) il contrasto la disinformazione.

Su tali premesse, ed è senz'altro questo il punto di maggiore interesse contenuto nel documento, la Strategia nazionale ha previsto tre obiettivi (protezione, risposta e sviluppo) accompagnati da un Piano di Implementazione composto di 82 misure specifiche contenenti indicazioni puntuali circa il ruolo degli attori responsabili e gli altri soggetti interessati. Ragioni di completezza della trattazione suggeriscono dunque di soffermarsi brevemente sul contenuto di ogni singolo obiettivo, in modo da poter successivamente fornire un'analisi complessiva delle diverse misure contenute nel Piano di Implementazione della strategia.

Il primo obiettivo (dedicato alla "protezione") è riferito all'esigenza di tutelare gli asset strategici nazionali attraverso un approccio sistemico orientato alla gestione e mitigazione del rischio di incidenti cibernetici. Tra i diversi interventi suggeriti per il perseguimento di tale obiettivo, tra cui figura il potenziamento delle capacità del CVCN e dei Centri di Valutazione istituiti presso il Ministero dell'interno e della difesa, meritano una particolare considerazione alcune questioni. Con riferimento al tema del mantenimento di un quadro giuridico nazionale aggiornato e coerente in materia di cybersicurezza, si è messo in chiaro come il solo costante aggiornamento della disciplina contenuta in fonte primaria sia oggi una condizione necessaria ma non sufficiente per la protezione degli asset strategici del paese. Infatti, oltre alla meticolosa costruzione di

un'efficiente intelaiatura normativa, risulta indispensabile la diffusione di linee guida basate su un approccio "*zero trust*" nonché lo sviluppo policy settoriali rivolte ai soggetti pubblici e privati coinvolti nell'ecosistema nazionale di cybersicurezza. Tra gli altri interventi richiesti dall'obiettivo "protezione" assume rilievo il potenziamento del livello di maturità delle capacità cyber della Pubblica Amministrazione attraverso la transizione sia verso il Cloud della Pubblica Amministrazione, sia verso tecnologie di Public Cloud. In tale contesto assume un rilievo centrale la creazione del Polo Strategico Nazionale (PSN) condotta dal Dipartimento per la trasformazione digitale con l'obiettivo di portare il 75% delle amministrazioni italiane ad utilizzare servizi *in cloud* entro il 2026.

Il secondo obiettivo (dedicato alla "risposta") ha inteso potenziare le capacità nazionali e transnazionali di monitoraggio, rilevamento, analisi e risposta di tutti gli attori coinvolti nell'ecosistema. Oltre a suggerire l'integrazione dei servizi cyber nazionali in alcuni ambiti specifici, tale sezione del documento ha permesso di fare chiarezza sulla distribuzione di competenze in materia di gestione degli incidenti e delle crisi di cybersicurezza ideato sulla base della piattaforma elaborata dalla Raccomandazione UE 2017/1584 (c.d. Blueprint). La strategia ha così ricostruito i diversi livelli dell'architettura di gestione degli incidenti informatici (politico, operativo e tecnico), in cui il vertice è affidato Presidente del Consiglio dei ministri, dall'autorità delegata per la sicurezza della Repubblica e al CISR e i due successivi livelli sono affidati rispettivamente al NCS e al CSIRT Italia. Sul versante transnazionale, invece, l'assetto disegnato si completa con il ruolo di collegamento che quest'ultima assicura con l'Unione Europea in caso di crisi o incidenti cyber transfrontalieri su larga scala in qualità di componente della rete CyCLONe[56] e della rete europea degli CSIRT.

56 La CyCLONe (Cyber Crisis Liaison Organization Network) è una rete lanciata in occasione della Blue OLEx, un'esercitazione europea di cybersecurity a livello operativo promossa dall'ENISA e dalla Commissione Europea nel 2020, con l'intento di rispondere in maniera tempestiva ed efficace ad ogni tipologia di attacco informatico su larga scala.

Nel terzo e ultimo obiettivo (dedicato allo "sviluppo") viene sottolineata l'esigenza di implementare il settore della tecnologia digitale mediante un'azione congiunta volta a includere i centri di eccellenza, le imprese più virtuose e l'accademia, facendo così emergere l'approccio «whole of society» perseguito dalla strategia. L'attore protagonista di per la realizzazione di tale obiettivo è nuovamente l'ACN, la quale rappresenta il Centro Nazionale di Coordinamento (NCC) chiamato a supportare, in stretto raccordo con il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca (ECCC), lo sviluppo dell'autonomia tecnologica e digitale italiana ed europea. Tra le iniziative più virtuose inserite in tale obiettivo va evidenziata la proposta di realizzare un "parco nazionale della cybersicurezza" destinato a ridurre la dipendenza del nostro paese da tecnologie *extra*-UE, ossia una struttura provvista di tutte le dotazioni tecnologiche necessarie per inglobare le numerose competenze e risorse provenienti dalla Pubblica Amministrazione, dal tessuto produttivo e dal mondo dell'accademia.

Come già anticipato, ciascuno degli obiettivi fin qui descritti è stato sviluppato nel Piano di Implementazione allegato alla strategia nazionale di cybersicurezza, il quale ha indicato in modo puntuale le organizzazioni responsabili e gli altri soggetti interessati per ognuna delle 82 misure contenute. La pubblicazione della strategia ha così permesso di introdurre una vera e propria distribuzione di competenze sul piano strategico, tecnico ed operativo tra tutti i soggetti coinvolti nell'ecosistema di sicurezza cibernetica. Osservando tale distribuzione da un punto di vista meramente quantitativo emerge come l'introduzione dell'Agenzia Nazionale abbia radicalmente trasformato la precedente architettura nazionale di cybersicurezza: solo quest'ultima risulta infatti direttamente responsabile della realizzazione di 66 misure (e figura quale soggetto interessato rispetto ad altre 11) mentre il Presidente del Consiglio dei ministri risulta responsabile solo in relazione a due misure (e neppure in via esclusiva). Sulla stessa linea, risulta meritevole di attenzione la posizione affidata dal Piano

di Implementazione agli operatori privati: questi ultimi risultano coinvolti nella realizzazione di ben 27 misure divenendo così il primo soggetto per quantità di ruoli attribuiti quale "interessato".[57]

L'analisi del contenuto della strategia non potrebbe dirsi conclusa in assenza di un riferimento al programma di investimenti necessario per la realizzazione degli ambiziosi obiettivi prefissati. Occorre infatti sottolineare che il primo punto della strategia nazionale ha destinato una quota percentuale dell'1,2% degli investimenti nazionali lordi su base annuale a specifiche progettualità volte a conseguire una piena autonomia tecnologica in ambito digitale e un ulteriore innalzamento dei livelli di cyber-sicurezza dei sistemi informativi nazionali[58]. A tali investimenti, al di là degli strumenti finanziari ordinari già assegnati alle Amministrazioni con competenza in materia *cyber*, occorre aggiungere i finanziamenti previsti dal PNNR nel settore relativo alla Digitalizzazione, Innovazione, Competitività, Cultura e Turismo. In tale ambito, lo specifico investimento 1.5 "Cybersecurity" ha stanziato ben 623 milioni di euro per la realizzazione di specifiche progettualità per la creazione e lo sviluppo di servizi all'avanguardia per la gestione del rischio cyber secondo una precisa tripartizione[59]. L'utilizzo di queste risorse è risulta tuttavia subordinato al rispetto di una serie di scadenze concordate con l'UE distribuite tra la fine del 2022 e la fine

57 Per un approfondimento volto a evidenziare l'importanza del ruolo degli operatori privati nell'attuale infrastruttura italiana di cybersicurezza si rimanda all'attenta analisi di L. PREVITI, *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, in *Federalismi.it*, 25, 2022, 65 ss.

58 Inoltre, essendo l'Agenzia designata quale Centro Nazionale di Coordinamento ex art. 6 del regolamento 2021/887 UE, l'Italia beneficerà di ulteriori finanziamenti provenienti dai programmi Orizzonte Europa ed Europa Digitale.

59 La prima area di intervento (174 milioni di euro) ha ad oggetto il raggiungimento della piena operatività dell'agenzia e la realizzazione di reti e servizi volti a potenziare le capacità nazionali di prevenzione, monitoraggio e risposta di minacci cibernetiche. La seconda area di intervento (301,7 milioni di euro) è stata dedicata interamente al potenziamento della resilienza cyber della Pubblica Amministrazione, ritenendo quest'ultima la chiave per una sicura transizione digitale del paese. La terza e ultima area (147,3 milioni di euro) guarda invece più da vicino il mondo privato dell'industria e dell'accademia, ponendo come obiettivo il raggiungimento di un'autonomia tecnologica nazionale che passa necessariamente dalle capacità nazionali di scrutinio e certificazione tecnologica.

del 2024[60], così gli ambiziosi obiettivi individuati dalla strategia non possono che segnare il punto di inizio di un percorso tortuoso che vedrà impegnata l'Italia, con a fianco l'Unione, nelle sfide del nuovo millennio.

7. La visione strategica dell'Italia tra realtà e mito

La vastità di temi e obiettivi presi in considerazione dalla Strategia Nazionale di Cybersicurezza 2022-2026 rende estremamente difficile formulare un giudizio complessivo circa suo contenuto.

Con riferimento ai numerosi obiettivi prefissati, il documento sembra aver offerto un importante contributo, proponendo numerose misure idonee a garantire un'accelerazione verso una transizione digitale cyber-resiliente della Pubblica Amministrazione e un modello di gestione di crisi cibernetiche multilivello di maggiore efficienza. Tra le misure più virtuose merita una particolare menzione la scelta di introdurre all'interno della strategia una specifica indicazione dedicata alla promozione cultura della sicurezza cibernetica volta ad accrescere la consapevolezza dei cittadini – con particolare riferimento ad alcune categorie di dipendenti pubblici, quali i magistrati – sui rischi derivanti dall'uso delle tecnologie informatiche. Infatti, la realizzazione di un'architettura istituzionale di difesa provvista di adeguati mezzi e competenze per fronteggiare le sempre più crescenti minacce cibernetiche non potrà dirsi di per sé idonea al raggiungimento degli obiettivi prefissati in assenza di un'adeguata valorizzazione del capitale umano.

---

60 Più in particolare, tra le scadenze europee fissate al 2022 figura il dispiego iniziale dei servizi nazionali di cybersecurity (in corso), l'avvio della rete dei laboratori di *screening* e certificazione della cybersecurity (in corso) e l'attivazione di un'unità centrale di audit per le misure di sicurezza PSNC e NIS (in corso); mentre tra le scadenze fissate per il 2024 figura il dispiego integrale dei servizi nazionali di cybersecurity (da avviare), il completamento della rete dei laboratori e dei centri di valutazione per la valutazione e certificazione della cybersecurity (da avviare) e la piena operatività dell'unità di audit per le misure di sicurezza PSNC e NIS con il completamento di almeno 30 ispezioni (da avviare). Per un approfondimento circa il contenuto dei singoli interventi si rimanda alla specifica sezione "cybersecurity" tra le misure monitorate su www.openpnrr.it.

Osservando i dati riportati dal più recente *Digital Economy and Society Index*[61] emerge come, tra l'87% dei cittadini europei attivi su internet, solo il 54% sia in possesso delle *digital skills* necessarie per poter navigare con sicurezza in rete. Il dato più preoccupante non è tanto relativo alla media europea, già di per sé indicativa dell'importanza della questione trattata, ma – per quel che riguarda la posizione strategica del nostro paese – al fatto che l'Italia si trovi tra gli ultimi posti di tale ingloriosa classifica seguita da Polonia, Bulgaria e Romania. Su tali premesse, essendo ormai noto che una parte significativa degli incidenti informatici avvenuti in Italia sia riconducibile più a disattenzioni umane che ad attacchi ben calibrati, la strategia ha sottolineato la necessità di un consistente investimento volto a offrire una soluzione su questo fronte (o almeno dei progressi significativi)[62]. Del resto, come evidenziato dalla dottrina più avveduta, soltanto il raggiungimento di una "immunità di gregge" basata sulla conoscenza dei sistemi può condurre il rischio *cyber* al di sotto di livelli accattabili[63].

Il raggiungimento nel medio termine di altri importanti obiettivi prefissati dalla Strategia appare tuttavia di difficile realizzazione, su tutti il conseguimento di una piena autonomia strategica ed europea nel settore tecnologico. Se è infatti vero che è possibile ridurre in modo significativo le forniture digitali di altri Stati *extra* UE attraverso lo sviluppo di tecnologie *disruptive* di matrice esclusivamente europea[64], il raggiungimento di una effettiva "sovranità digitale"

---

61 *Digital Economy and Society Index Report 2022*, reperibile su https://digital-strategy.ec.europa.eu/en/policies/desi-human-capital.

62 La questione è stata affrontata negli stessi termini da R. Brighi, P.G. Chiara, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in *Federalismi.it*, 21, 2021, 18-42;

63 Il concetto è espresso e meglio approfondito e P. L. Montessoro, *Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale*, in *IdF*, 3, 2019, 783-800.

64 Il termine *disruptive technologies* è stato coniato nel 1995 da Clayton Christensen per fare riferimento a quell'insieme di nuove tecnologie che, in ragione della loro componente innovativa, sono capaci di modificare completamente la logica fino a quel momento presente nel mercato (J. L. Bower, C. M. Christensen, *Disruptive tecnologies: catching the wave*, in *Harvard Business Review*, January-February, 1995, 43-53). Senza alcuna pretesa di esaustività, tra le principali tecnologie ad oggi considerate *disruptive* possono ricordarsi quelle relative a: big data, intelligenza artificiale, blockchain, tecnologie dell'Internet of Things (IoT) e 5G e al *quantum computing*.

europea – e men che meno italiana – rimane ancora ad oggi un vero e proprio mito a causa della scarsa reperibilità di materie e della irrinunciabile dipendenza da Paesi che si trovano in contesti geopolitici imprevedibili e complessi (basti pensare che il 98% dei materiali semiconduttori utilizzati in Europa deriva da Taiwan).

Ciò non vuol dire che le istituzioni dell'Unione non stiano provando, seppure con un ritardo ventennale[65], a ridurre il rapporto di dipendenza di approvvigionamento di materie prime critiche da partner non affidabili. La recente carenza di semiconduttori a livello mondiale (c.d. *chip crunch*)[66] ha infatti condotto la Commissione a disegnare una strategia per raddoppiare la produzione di chip "made in UE" entro il 2030 attraverso investimenti pubblici e privati per circa 43 miliardi di euro[67]. Sarebbe tuttavia illusivo ritenere (l'auspicato) raggiungimento di questi obiettivi sufficiente per garantire all'UE una futura posizione di *leadership* nel settore, dal momento che neppure gli Stati che negli ultimi decenni hanno più investito su questo fronte (Cina e USA) hanno ad oggi il controllo completo della filiera di ricerca e produzione dei semiconduttori.

---

65 Secondo i dati del recente report offerto da Kearney (*Europe's urgent need to invest in a leading-edge semiconductor ecosystem*, 2022) l'Unione Europea nel 2000 produceva circa il 25% dei semiconduttori a livello globale, mentre oggi la quota è vicina al 9%. Il dato più preoccupante va tuttavia riferito alla produzione di semiconduttori all'avanguardia, in cui nello stesso intervallo di tempo la produzione è passata dal 19% a una percentuale vicina allo 0. Secondo il report citato, la causa principale di tale parabola discendente è riconducibile alla mancata adozione di adeguate misure comunitarie dirette ad agevolare la competizione tra le principali aziende europee di allora (Siemens, Ericsson e Nokia) e i *players* americani e asiatici.

66 L'attuale crisi che ha colpito il mercato di chips e semiconduttori può ritenersi causa del combinarsi di numerosi fattori eterogenei: l'iniziale impennata della domanda causata dagli isolamenti imposti in tutto il mondo per il contenimento del COVID-19, la chiusura di alcuni stabilimenti e la riduzione della capacità di estrazione di materie prime di Taiwan, le tensioni commerciali tra USA e Cina e, da ultimo, l'avvio della guerra tra Ucraina (principale esportatore del gas neon utilizzato per l'incisione dei chip) e Russia (detentore di circa un terzo del palladio disponibile sul mercato).

67 Si fa riferimento al "*Chips Act*", ossia il pacchetto legislativo europeo sui semiconduttori contenente una comunicazione, una proposta di regolamento e una raccomandazione approvato l'8 febbraio 2022 dalla Commissione europea e attualmente al vaglio del Parlamento.

Oltre agli interrogativi fin qui sollevati in relazione alla "sovranità digitale" italiana ed europea, sorgono alcuni dubbi anche in relazione all'approccio utilizzato dalla strategia in materia di contrasto a campagne mirate di disinformazione online *state sponsored* (rientrando nel più ampio tema della c.d. *information warfare*)[68]. In un primo momento il documento ha infatti inserito tra le sue principali sfide quella di individuare meccanismi di difesa idonei a prevenire interferenze di altri al libero svolgimento di processi politici interni tramite meccanismi di disinformazione, ma non può dirsi che la stessa attenzione sull'argomento sia poi stata mantenuta nell'elaborazione di soluzioni efficaci per affrontare un tema di così ampia portata. In particolare, il tema del contrasto alla disinformazione online è racchiuso in un'unica e generica misura del Piano di Implementazione della Strategia con cui si è suggerita una non meglio specificata azione di coordinamento nazionale ed europeo "anche attraverso campagne informative" rivolte ai cittadini. Iniziativa, quest'ultima, che non può di certo ritenersi sufficiente per affrontare la complessità e la vastità del fenomeno descritto.

Le critiche fin qui espresse circa alcuni profili della strategia vanno tuttavia tenute in considerazione con le dovute cautele e non possono in ogni caso mettere in ombra il contributo offerto da tale documento in termini di sviluppo dell'ecosistema di cybersicurezza. La Strategia Nazionale è pur sempre un atto programmatico che dovrà essere tradotto in legge nel corso del prossimo quinquennio attraverso degli interventi che richiederanno il supporto di numerose competenze specialistiche. Dunque, nel futuro non mancheranno di certo occasioni per ricalibrare le priorità imposte dalla costante evoluzione tecnologica e implementare via via la qualità delle misure richieste per raggiungere i traguardi desiderati.

---

68 Per una panoramica generale, tra le sterminata letteratura sull'argomento, si rimanda a J. Aro, *The cyberspace war: propaganda and trolling as warfare tools*, in *European view*, 1, 2016, 121-132; M. Cavino, *Il triceratopo di Spielberg. Fake news, diritto e politica*, in *Federalismi.it*, 11, 2020, 32-42; C. Valditara, *Fake news: regolamentazione e rimedi*, in *Dir. inf.*, 2, 2021, 257-282.