Il Mulino - Rivisteweb

Giuseppe Borriello, Gaia Fristachi

Stato (d'assedio) digitale e strategia italiana di cybersicurezza

(doi: 10.53227/105071)

Rivista di Digital Politics (ISSN 2785-0072)
Fascicolo 1-2, gennaio-agosto 2022

Ente di afferenza:
()

Copyright © by Società editrice il Mulino, Bologna. Tutti i diritti sono riservati.
Per altre informazioni si veda https://www.rivisteweb.it

Licenza d'uso

Questo articolo è reso disponibile con licenza CC BY NC ND. Per altre informazioni si veda https://www.rivisteweb.it/

Giuseppe Borriello, Gaia Fristachi

Stato (d'assedio) digitale e strategia italiana di cybersicurezza

DIGITAL (SIEGE) STATE AND ITALIAN CYBERSECURITY STRATEGY

The increasingly massive affirmation of digital technologies in the public sector introduces important potential for improving public action, although it involves a whole series of security issues. The digital space is the new battlefield in which States play the game for sovereignty. The current historical contingencies push Nations towards a new digital arms race. Over the last few years, Europe, to carve out a leading international role, has displayed increasing attention on the defense and digital security sector. Italy, for its part, is responding to EU input, and trying to take steps forward regarding cybersecurity. The Italian commitment is embodied in a new political awareness of the issue. This effort consists in a first major public investment and in the reorganization of the institutional structure. Cyberspace has never before been a policy priority like it is today, as demonstrated by the pandemic crisis and the outbreak of recent international conflicts, the importance of which is expected to increase even further in the near future.

KEYWORDS *Cybersecurity, Cyberwar, Sovereignty, European Scenario, Italy.*

1. Introduzione

«L'unico computer sicuro è uno che sia stato spento, sepolto da una colata di cemento e sigillato in una stanza dalle pareti foderate in piombo, protetta da guardie armate. E anche in quel caso, ho dei dubbi» (Spafford 1989, 110). Le parole dello studioso americano Gene Spafford indicano chiaramente che è utopico immaginare un sistema informatico esente da qualsivoglia rischio o minaccia, a prescindere dalle condizioni contestuali nel quale esso viene a

Giuseppe Borriello, Dipartimento di Scienze Sociali, Università degli Studi di Napoli Federico II – Vico Monte della Pietà, 1 – 80138 Napoli, email: giuseppe.borriello@unina.it, orcid: 0000-0001-9740-6186.

Gaia Fristachi, Dipartimento di Scienze Politiche, Università degli Studi di Napoli Federico II – Via Leopoldo Rodinò, 22 – 80133 Napoli, email: gaia.fristachi@unina.it, orcid: 0000-0002-9669-6748.

ISSN 2785-0072
© Società editrice il Mulino

collocarsi. Ad oggi sono più di 30 milioni le identità digitali (Spid) emesse[1], oltre 60 milioni i cittadini censiti presso l'Anagrafe nazionale della popolazione residente (Anpr)[2] e circa 440 milioni le transazioni PagoPa registrate a partire dal 2016, il cui controvalore economico raggiunge quasi gli 80 miliardi di euro[3]. Questi sono solo alcuni dei numeri che testimoniano la portata dello tsunami web-digitale (Calise e Musella 2019) che ha investito il settore pubblico italiano nel corso degli ultimi anni. Tuttavia, la staticità temporale di tali dati si accompagna a un trend di costante crescita nel tempo.

Se da un lato l'implementazione delle politiche di e-government, l'affermazione degli algoritmi, dei big data e dell'intelligenza artificiale hanno favorito la velocizzazione delle prestazioni del settore pubblico, dall'altro si sta determinando un rimodellamento dei tradizionali sistemi di partecipazione democratica. Tuttavia, l'applicazione del potenziale tecnologico all'azione umana non si caratterizza per i suoi soli vantaggi, bensì comporta anche dei costi ed evidenzia l'emersione di nuove vulnerabilità, esposte alle dannose intenzioni di taluni attori. Difatti la crisi pandemica internazionale ha gettato luce sulle disfunzioni attribuibili al mondo digitale: lo spostamento nella realtà virtuale delle tradizionali attività quotidiane ha dato luogo ad un vero e proprio cambio di paradigma per le operazioni criminali, orientate a violare i sistemi meno raffinati di protezione informatica delle organizzazioni aziendali e pubbliche (European cyber security organisation 2020a; Ramadan *et al.* 2021). Parallelamente lo scoppio del conflitto russo-ucraino ha allertato i leader mondiali, instillando il timore dell'avanzamento di una imminente guerra, non più soltanto militare ma anche cibernetica, suscettibile di generare una vera e propria paralisi del sistema geopolitico mondiale. Pertanto, le preoccupazioni in materia di cybersecurity sono divenute dei veri e propri problemi di sicurezza nazionale (Kemmerer 2003). Lo spazio cibernetico non è, infatti, escluso dalle logiche geopolitiche e della competizione internazionale, anzi l'utilizzo della tecnologia digitale apre nuovi ed impensabili scenari di ingerenza negli affari interni di uno Stato, che impattano fortemente sul principio di sovranità, in ragione dell'enorme propagazione di quello che è stato definito il «virus digitale» (Calise 2021).

In questo tormentato contesto, in un'ottica di azione multilivello, si pone dunque il ruolo dell'Unione europea. Quest'ultima ha scelto infatti di adottare una propria strategia di prevenzione e difesa in ambito comunitario, ispirandosi al percorso statunitense. Malgrado ciò, nell'ultimo decennio la politica di euro-cybersicurezza è cambiata notevolmente, sia per quanto riguar-

[1] Fonte: https://avanzamentodigitale.italia.it/it/progetto/spid.
[2] Fonte: https://avanzamentodigitale.italia.it/it/progetto/anpr.
[3] Fonte: https://avanzamentodigitale.italia.it/it/progetto/pagopa.

da gli obiettivi a cui essa fa riferimento, sia per quel che concerne il livello di priorità ad essi attribuito (Kasper 2020). Tale repentino mutamento, generato anche dalla freneticità dell'avanzamento digitale, si è dovuto tuttavia scontrare con la consueta lentezza burocratica degli interventi statali. Pertanto, in questo contesto si inserisce il caso italiano, caratterizzato da un cronico ritardo in tema digitale (Commissione europea 2021), in cui l'evoluzione della policy segna un passaggio da una governance frammentata ad una maggiormente accentrata attorno alla nuova Agenzia nazionale per la cybersecurity.

Il presente contributo si pone dunque l'obiettivo di fare il punto su tre insight tematici: in primo luogo si analizzerà, sotto il profilo epistemologico storico-evolutivo, il significato attribuito al termine cybersecurity, tenuto conto della sua particolare attrattività contemporanea. Successivamente verranno ripercorse le tappe più significative del tracciato politico europeo in tema di sicurezza informatica. Infine, si effettuerà una ricognizione dei rischi a cui è sottoposto il sistema informatico del settore pubblico italiano, per poi giungere ad una ricostruzione della strategia di sicurezza digitale perseguita dall'Italia.

Ora, sebbene le minacce informatiche non abbiano l'immagine drammatica di una bomba che esplode o di un aereo dirottato volto a schiantarsi contro un edificio, esse sono comunque suscettibili di danneggiare gravemente i servizi governativi e le attività commerciali, di bloccare i sistemi di comunicazione elettronici e di minare la fiducia – oramai già fortemente compromessa – che i cittadini ripongono nelle istituzioni pubbliche (Ciolan 2014). Emerge dunque chiaramente che, nell'era dell'interconnessione fra luoghi e dell'interdipendenza tra attori, specialmente in una fase critica come quella odierna, la cybersecurity rappresenta un bene pubblico da non sottostimare.

2. Cyber + sicurezza: modellare il futuro dell'Europa digitale

In un mondo globalizzato e sempre più interconnesso come quello odierno è divenuto oramai impensabile vivere separati dai propri dispositivi elettronici o semplicemente resistere alla tendenza a diffondere attraverso di essi una miriade di dati informativi, spesso molto personali e sensibili. La dipendenza umana dallo spazio digitale è infatti resa appetibile dalle caratteristiche proprie di questo cyber-substrato, rappresentate dalla velocità, dall'anonimità e dall'economicità dell'informazione. Tuttavia, altrettanto istantaneamente, queste stesse prerogative sono suscettibili di trasformarsi in potenziali punti di debolezza del sistema cibernetico, esponendo dati ed individui a pericolose violazioni. Per tale ragione, numerosi studiosi, professionisti e politici hanno

fatto sempre maggiore ricorso al termine «cybersecurity» o, più in generale, all'espressione «sicurezza informatica». Tuttavia, a dispetto della sua rilevanza strategica per la sicurezza nazionale ed internazionale, ancora oggi sembrerebbe esservi una scarsa comprensione delle implicazioni pratiche, potenzialmente distruttive, connesse a tale fenomeno.

Invero il termine «cybersicurezza» ha radici storiche lontane poiché il suo primo utilizzo letterale risale probabilmente al 1989, dunque ben dopo l'affermazione della scienza cibernetica e della sua applicazione nel campo della governance umana (Williams 2020). Tradizionalmente tale terminologia viene ricollegata al mondo delle tecnologie dell'informazione e della comunicazione e alle sue diverse sub-aree. Tuttavia, secondo gli studiosi delle scienze sociali, questa locuzione non può essere analizzata prescindendo dal contesto giuridico e sociale nella quale viene a collocarsi. Pertanto, questa visione ambivalente è rappresentativa del fatto che la sicurezza informatica è da considerarsi un tema multidisciplinare, ricco di sfaccettature e regolamentabile soltanto in un'ottica multilivello integrata. Difatti, al pari dell'avanzamento tecnologico, la cybersicurezza è un campo soggetto ad un repentino aggiornamento che, a sua volta, trascina con sé anche i propri fondamenti lessicologici (Lanza e Daille 2019). Proprio a causa di questa sua natura dinamica, è difficile rinvenire in letteratura scientifica una definizione univoca di cybersecurity. Craigen, Daikun-Thibault e Purse (2014) sono stati tra i primi a riconoscere che la sicurezza informatica è in realtà un «termine mal definito». L'ampiezza del settore al quale viene fatto riferimento comporta infatti l'intersezione di una pluralità di discipline e approcci differenti, i quali conducono spesso a definizioni fortemente variabili, soggettive e talvolta non informative. L'elemento tecnico ostacola così il metodo delle scienze storico-sociali e viceversa, impedendo un raffronto di visioni che potrebbe invece risultare cruciale per la risoluzione dei problemi odierni, connessi alle sfide poste dall'innovazione tecnologica (Peslak e Hunsinger 2019).

Il primo passo per comprendere appieno le caratteristiche della cybersicurezza deve essere dunque di tipo terminologico: si rende pertanto necessario esaminare la funzione di questo settore, individuando precipuamente cosa si ritiene meritevole di protezione. A questo proposito, la commistione tra l'approccio ascrivibile alle scienze tecnico-informatiche ed il criterio di analisi delle scienze politiche e sociali consente di pervenire ad una definizione più o meno onnicomprensiva del fenomeno. Il termine «cybersecurity» viene infatti qui inteso come quell'insieme di misure che le istituzioni pubbliche adottano nel tentativo di tutelare i sistemi informatici e gli individui, che interagiscono nel dominio del cyberspazio, da eventuali attacchi malevoli. Non rileva ai fini dell'applicazione della definizione qui in esame se tali attacchi siano da con-

siderarsi delle attività volontarie o meramente accidentali. Sebbene in taluni casi il concetto di sicurezza informatica venga sovrapposto a quello di sicurezza delle informazioni (Schatz *et al.* 2017), preme sottolineare che la seconda categoria si rapporta alla prima in termini di spècies a gènus, costituendo essa una mera specificazione della prima, nella quale viene ricompresa a tutti gli effetti. Accanto ad essa si pongono infatti tutta una serie di potenziali minacce di differente natura, tra le quali vengono tradizionalmente ricomprese l'hacktivismo, il cyberterrorismo, lo spionaggio informatico e, più in generale, la guerra cibernetica. Avere una panoramica chiara delle sfide dinanzi le quali si gioca il dominio del potere statale è infatti cruciale, da un lato, per preservare adeguatamente la privacy dei cittadini e dall'altro, per tutelare l'integrità dei sistemi nazionali. Tuttavia, in assenza di un approccio terminologico ed operativo concordato, è chiaro che l'ambizione di pervenire ad un sistema integrato di cyber-governance rimane tutt'oggi molto distante (Schatz *et al.* 2017).

A questo proposito uno sforzo apprezzabile di sistematizzazione teorica e pratica è da ascriversi all'Unione europea: difatti è proprio nel 2013, in concomitanza con l'affermazione delle cosiddette rivelazioni Snowden e in occasione dell'approvazione della Strategia Ue per la cybersicurezza, che tale organizzazione sovranazionale fornisce per la prima volta nella storia una propria definizione di sicurezza informatica, secondo cui essa «si riferisce comunemente alla salvaguardia e alle azioni che possono essere utilizzate per proteggere il dominio cyber, sia in campo civile che militare, da quelle minacce che sono associate o che possono danneggiare le sue reti ed infrastrutture informatiche interdipendenti. La sicurezza informatica si impegna a preservare la disponibilità e l'integrità delle reti e delle infrastrutture e la riservatezza delle informazioni in esse contenute» (Kasper 2020, 169). Come evidente, almeno in un primo momento, il focus tematico di tale definizione si limiterà a considerare quelli che sono gli aspetti puramente tecnico-operativi dei sistemi informatici. Tuttavia, successivamente, con l'emanazione del Cybersecurity act del 2019, le istituzioni europee sceglieranno di ampliare tale enunciazione, sino ad includere in essa la tutela dei cittadini europei poiché, in quanto utenti digitali, sono da considerarsi potenziali vittime di minacce informatiche.

Eppure, l'interesse europeo a circoscrivere il fenomeno cyber non emerge inaspettatamente dall'oggi al domani. Invero la necessità di regolamentare questo nuovo spazio di azione statale viene riconosciuta già nei primissimi anni Duemila. Il programma riformista dell'Ue, ispirato all'attuazione della Strategia di Lisbona, riconosce infatti il ruolo preponderante dell'economia digitale. Pertanto, sulla scorta di questa agnizione, viene lanciata nel 2010 l'Agenda digitale europea: quest'ultima ha durata decennale ed è volta all'affermazione di un mercato unico digitale in cui cittadini ed imprese dispongono

del libero accesso ed operano secondo logiche eque. Un biennio più tardi, per volontà della Commissione europea, è stato istituito il *Computer emergency response team* (Cert-Eu), ossia un team permanente di risposta alle emergenze informatiche, composto da esperti provenienti dalle principali istituzioni europee. Oggigiorno esso funge da hub di coordinamento tra i diversi *Computer security incident response team* (Csirt) nazionali e collabora attivamente con le principali società specializzate in sicurezza informatica, svolgendo così un ruolo chiave in termini di prevenzione, rilevazione e contrasto di attacchi e/o incidenti informatici.

Ora, sebbene l'Ue, a modo suo, abbia compiuto dei significativi passi avanti in termini di cybersicurezza, è il 2013 a costituire l'anno spartiacque in termini di avanzamento cibernetico a livello comunitario: in quell'anno, infatti, viene compiutamente presentata per la prima volta una strategia europea per la sicurezza informatica, successivamente aggiornata nel 2017. Nell'ambito di questo programma è stato poi diramato il regolamento (Ue) 526/2013, attraverso cui la Commissione ha scelto di estendere (fino al 2020) e rafforzare il mandato dell'Agenzia Ue per la cybersicurezza (Enisa), istituita nel 2004, rendendo così quest'ultima un vero e proprio punto di riferimento europeo in termini di sicurezza informatica (Schlehahn 2020). L'anno successivo, sulla scorta delle conclusioni adottate dal Consiglio europeo sulla politica di sicurezza e di difesa comune, il Consiglio Ue ha predisposto la definizione di un framework politico in materia di protezione informatica, aggiornato poi nel 2018 (European court of auditors 2019). Quest'ultimo ha pertanto individuato ben cinque aree prioritarie di intervento, rappresentate rispettivamente dalla: 1) necessità di rafforzare le capacità di cyberdifesa dei diversi paesi europei; 2) irrobustire i livelli di protezione delle reti di comunicazione e informazione della politica europea di sicurezza e di difesa comune (Pesd); 3) promuovere la cooperazione civile e militare con riferimento alle politiche informatiche sull'intero territorio dell'Unione; 4) garantire maggiori opportunità di istruzione e formazione digitale e infine 5) rinvigorire i rapporti con i principali partner internazionali competenti in materia (prestando una particolare attenzione ai rapporti intrattenuti con la Nato). L'attuazione di tali macro-obiettivi era poi collegata alla fase operativa, per la quale si distinguevano oltre quaranta proposte.

Nel 2016 è poi intervenuta la direttiva (Ue) *Network and information security* (Nis) 2016/1148, volta ad incrementare il livello di sicurezza delle reti e dei sistemi informativi rientranti nell'orbita europea (Markopoulou *et al.* 2019). Scopo principale di tale atto giuridico è di far sì che tutti gli Stati dell'Unione, attraverso l'adozione di proprie strategie in campo nazionale, siano messi in condizione di gestire e reagire – attraverso il recupero dei servizi – a potenziali attacchi cibernetici distruttivi. A tal proposito vengono indivi-

duati dei settori strategici di riferimento, tra i quali rientrano quello energetico, dei trasporti, della Sanità, ecc. In particolare, l'Italia ha recepito tale direttiva con l'adozione del Dlgs n. 65/2018, scegliendo però di estendere il perimetro di riferimento previsto a livello comunitario e di attribuire al Dipartimento delle Informazioni per la Sicurezza un ruolo di primo piano in termini di coordinamento interno. Parimenti, nel 2017, l'Ue ha deciso di dotarsi di una «cassetta degli attrezzi» (*Eu cyber diplomacy toolbox*) per difendersi da potenziali azioni malevoli poste in essere nel perimetro dello spazio cibernetico europeo. Questo kit di strumenti prevede inoltre la possibilità di imporre, nel rispetto dei limiti previsti dal principio di proporzionalità, delle misure restrittive nei confronti dei malintenzionati. Trattasi dunque di uno sforzo diplomatico coordinato, le cui specifiche sono però ancora in fase di definizione.

Infine, sempre nel tentativo ambizioso di plasmare il futuro digitale dell'Europa, l'Ue ha recentemente adottato il regolamento 2019/881, noto come Cybersecurity act. Quest'ultimo propende ad un duplice intento: da un lato, si consolida il ruolo tecnico e operativo attribuito all'Enisa, attraverso il conferimento a quest'ultima di un mandato permanente; dall'altro, invece, viene fissato un quadro europeo delle certificazioni per la sicurezza informatica, individuando per la prima volta, nell'ambito del mercato digitale unico, degli standard comunitari di valutazione basati su tre livelli di cybersecurity (livello base, sostanziale o elevato). Tuttavia, l'avvento della crisi pandemica internazionale ha messo a dura prova gli avanzamenti compiuti dall'Ue in tema di sicurezza cibernetica, evidenziando così la necessità di accelerare l'impegno politico su alcuni nodi critici. Pertanto, nel novembre 2019, l'Agenzia Ue per la cybersicurezza ha presentato una relazione tecnica sulle minacce connesse allo sviluppo dei network 5g. In virtù delle criticità emerse nel documento, il gruppo di cooperazione Nis dell'Ue ha deciso di elaborare un apposito toolbox per garantire la sicurezza della rete 5g. Analogamente la scelta di revisionare i contenuti della precedente direttiva Nis ha costituito un ulteriore passo avanti per il continente europeo: ancora una volta l'elemento cardine è rappresentato dalla necessità di rendere i paesi europei resilienti sul piano digitale. Il Consiglio europeo ha pertanto ritenuto opportuno creare un'apposita unità informatica congiunta per sviluppare il toolbox sopra menzionato. Inoltre, sono stati stanziati enormi fondi per la programmazione del nuovo quadro finanziario pluriennale per un'Europa digitale (noto come Digital Europe 2021-2027) (European cyber security organisation 2020b). Infine, la Nis 2.0 si accompagna poi alla definizione del futuro *Cybersecurity resilience and semiconductor act*, da proporre nel corso del 2022 (European union agency for cybersecurity 2022).

L'intento politico è di definire una nuova strategia europea per la sicurezza informatica, che trova la propria ragion d'essere e la propria legittimazione politica nell'attuazione dell'obiettivo di transizione digitale individuato dal Recovery plan. A conti fatti, sebbene con qualche margine di ritardo rispetto ai paesi anglosassoni, l'Europa è riuscita a mettersi in corsa in campo digitale sul fronte Pesd e ad acquisire competitività cibernetica sul piano internazionale. In risposta ad un contesto geopolitico in continua evoluzione, la strategia europea per la cybersecurity, a partire dal 2013, ha quindi progressivamente consolidato, dal punto di vista terminologico e operativo, due aspetti centrali dell'impegno europeo: da un lato, ha rinsaldato politicamente in un framework univoco gli ambiti strategici nei quali viene a giocarsi la lotta per il potere digitale, dall'altro ha riconosciuto l'importanza del cyberspazio quale risorsa critica per il progresso economico. Infine, gli ultimi interventi in materia hanno rappresentato un passaggio politico significativo per l'armonizzazione delle policy tra Stati membri, transitando da un approccio lacunoso e disorganico ad un approccio integrato, tanto sul piano economico-commerciale quanto in ambito politico-militare.

3. Il contesto italiano

I numeri richiamati in apertura di questo articolo contribuiscono a testimoniare, da un lato, il ritmo incalzante della trasformazione digitale nel settore pubblico italiano, dall'altro, la portata empirica della sfida che rappresenta la difesa e la sicurezza dell'ambiente cibernetico, rendendo necessario predisporre adeguate precauzioni al fine di assicurare il corretto funzionamento dello Stato. Non a caso, circoscritta la definizione del fenomeno e introdotti quelli che sono gli input di matrice comunitaria, la diffusione delle tecnologie digitali nei meandri organizzativi del sistema amministrativo italiano e gli importanti investimenti previsti all'interno del Piano nazionale di ripresa e resilienza hanno imposto anche all'Italia di formulare un'efficace strategia di cybersicurezza nazionale. Nei fatti, l'esigenza di predisporre una strutturata policy in materia è divenuta sempre più incalzante in ragione delle criticità emerse con la pandemia, con l'implementazione dei servizi pubblici digitali (Sgueo 2022) e con la diffusione dello smart working nel settore pubblico (De Masi 2020; Istat 2021; Di Mascio *et al.* 2021), oltre che all'accentuarsi delle minacce alla sicurezza nazionale (Renzi 2021a; 2021b) provenienti da attori legati, direttamente o indirettamente, a Stati stranieri. Nei prossimi due paragrafi l'obiettivo sarà duplice. Da un lato si proverà a descrivere la portata empirica dei rischi e delle criticità che interessano il settore pubblico italiano, richiamando alcuni

dei più aggiornati report sul tema, come la Relazione annuale sulla politica per l'informazione e la sicurezza 2021 (Presidenza del Consiglio dei ministri 2022), i dati offerti dall'Istat (2021) e quelli derivanti dall'azione di monitoraggio dell'Agid (Cert-Agid 2021). Successivamente si cercherà di delineare gli interventi di policy perseguiti in materia di cybersicurezza al fine di chiarire quelli che risultano essere i principi guida della strategia italiana in materia (sul tema, Carotti 2020; Renzi 2021c; Renzi 2022).

Il punto di partenza per comprendere la portata del fenomeno risulta essere la ricognizione effettuata nell'ultima Relazione annuale sulla politica dell'informazione e della sicurezza per il 2021, presentata in Parlamento nel febbraio 2022. Nel documento si sottolinea come il perdurare dell'emergenza da Covid-19 e delle conseguenti misure di ampliamento delle attività svolte in formato digitale, sia nel settore pubblico che in quello privato, abbia imposto di mantenere alta l'attenzione nel dominio cyber al fine di garantire la tutela delle principali infrastrutture nazionali. Ciò che emerge dall'attività info-operativa condotta dall'intelligence risulta essere una generale crescita in termini assoluti delle azioni di minaccia cyber, le quali anche nel corso del 2021 (così come era successo per il 2020) hanno visto come principale bersaglio degli attacchi la Pubblica amministrazione, con il 69% del totale. Si registra, inoltre, un certo aumento anche per il settore privato (24% nel 2021 rispetto al 17% del 2020) testimoniando come, pur risultando tradizionalmente meno appetibile in virtù della strutturazione in piccole e medie imprese del tessuto economico italiano (Bozzetti *et al.* 2019), il fenomeno impatti ormai in modo generalizzato sull'intero sistema paese. Nel documento viene, inoltre, messa l'attenzione sui target specifici oggetto di attacchi contro la PA; le principali vittime sono state le amministrazioni centrali dello Stato (56%, un valore in aumento di 18 punti percentuali rispetto alla rilevazione 2020) e le infrastrutture digitali proprie di enti locali come regioni, province e comuni, (20%) oltre che le strutture del Servizio sanitario nazionale (10%).

Altro dato interessante che emerge dalla Relazione annuale riguarda le tipologie di attori coinvolti negli attacchi, delineando il profilo dei responsabili della minaccia digitale a cui sono sottoposti gli attori pubblici e privati. Essi, ove individuabili, rappresentano un'informazione preziosa che identifica al meglio la portata strategica e il valore geopolitico della cybersicurezza. Il 2021 ha, infatti, registrato un significativo aumento nell'individuazione delle responsabilità dell'offensiva digitale da parte di attori statuali dotati di quelle che nella relazione sono definite come vere e proprie «armi digitali» (si passa dal 5% del 2020 al 23% del 2021); essi agiscono al fine di sabotare attività produttive e occultare tracce di precedenti attività di spionaggio. Il dato, così come riportato nella relazione stessa e testimoniato dall'altalenante variazione

registrata nel triennio 2019-2021 (Tab. 1), risulta essere evidentemente sottostimato in ragione delle caratteristiche intrinseche all'ambiente digitale e delle tecnologie utilizzate negli attacchi, le quali agevolano l'anonimato e complicano la definizione certa di responsabilità. A tal riguardo significativo pare essere il dato del 40% degli attacchi registrati nel 2021, qualificati dall'intelligence come «non identificati», a riprova della complessità del tema e della difficoltà di ricostruirne una fedele rappresentazione. A questo si aggiunga il ricorso da parte degli Stati a gruppi di cyber-criminali e hacker indipendenti con l'obiettivo di delegare a questi l'esecuzione di operazioni di spionaggio e lo sviluppo di armi digitali, introducendo un ulteriore strato di anonimato nell'azione offensiva.

Tab. 1. *Attori responsabili dell'attacco (distribuzioni percentuali)*

Tipologia di attori	2019	2020	2021
Cyberespionage	12%	5%	23%
Criminalità	1%	4%	14%
Hacktivismo	73%	71%	23%
Non identificati	14%	20%	40%

Fonte: Relazione Annuale sulla Politica per l'Informazione (2021; 2020).

Se questo appare il quadro proposto dai dati, oltre a mettere in risalto l'attivismo di Stati terzi, il rapporto prodotto dall'intelligence cerca di porre l'attenzione su quelle che sono le finalità e gli esiti degli attacchi condotti. A conti fatti, la situazione che si presenta è quella di una ricostruzione opaca che riguarda sia le responsabilità che i fini, ma in cui si evidenzia l'esito certo di una grave violazione del principio di non ingerenza negli affari interni di uno Stato così come stabilito dall'art. 3 della Carta Onu. Nella relazione, infatti, da un lato emerge come in due casi su tre risulta difficile attribuire una chiara finalità all'attacco, anche perché spesso le azioni effettuate si classificano come prodromiche a potenziali attacchi mirati successivi; dall'altro si sottolinea come lo spazio cibernetico risulti essere un terreno privilegiato di una guerra che si combatte intorno al controllo dei dati e delle informazioni strategiche capaci di influenzare l'opinione pubblica, declinando quella che si prospetta come una minaccia senza precedenti al cuore dello Stato. Non a caso nel rapporto si parla di una sorta di minaccia ibrida: quest'ultima fa riferimento ad un'azione complessa che combina l'uso di tutti gli strumenti di ingerenza di cui dispone uno Stato sovrano (diplomatico, militare, economico, finanziario, di intelligence e informatico), mantenendoli al di sotto di una soglia rilevabile di responsabilità, con l'obiettivo di renderne opaca sia l'attribuzione della condotta ostile che la predisposizione di un'eventuale risposta (Presidenza del Consiglio

dei ministri 2022, 43). In questo senso, quindi, l'ambiente digitale si trasforma in un campo di battaglia privilegiato attraverso cui sfruttare le vulnerabilità del target. Il fine è quello di condizionarne i processi strategici come il decision making politico-amministrativo, l'esercizio del voto e la libertà di espressione. In questo contesto l'Italia non pare essere risparmiata da questo trend.

Se la Relazione annuale 2021 sulla politica dell'informazione per la sicurezza consente di mettere in evidenza la portata delle minacce a cui sono sottoposte le infrastrutture digitali del settore pubblico italiano, le rilevazioni dell'Istat e i monitoraggi Agid consentono di fare il punto su cosa le amministrazioni stanno facendo per fronteggiare tali pericoli.

Su questo fronte, emblematici appaiono i risultati che emergono dall'azione di monitoraggio effettuata dall'Agid in relazione allo stato di aggiornamento dei protocolli Https («Hypertext transfer protocol over secure socket layer») e dei Cms («Content management system») sui sistemi della PA (Cert-Agid 2021). Essi, pur non assicurando una esaustiva valutazione della sicurezza delle infrastrutture informatiche, rappresentano comunque due aspetti indicativi della diffusione di una cultura in materia di cybersicurezza rappresentativa del settore pubblico. Sul primo punto, l'analisi dei protocolli *https* effettuata dal raffronto dei due monitoraggi, svolti nel 2020 e 2021, registra un contesto in cui a prevalere è una situazione caratterizzata da un elevato numero di amministrazioni (circa il 53% nel 2021) caratterizzate dalla presenza di gravi problemi di sicurezza informatica. A rendere meno amara tale realtà è la constatazione che il dato risulta essere in miglioramento rispetto al 2020, quando le amministrazioni con gravi problemi di sicurezza erano addirittura il 67%, oltre al fatto che si registra un certo aumento dei soggetti che vengono considerati sicuri dagli esperti del Cert-Agid (il valore passa dal 9% del 2020 al 22% del 2021). Risultati più negativi si registrano invece nei livelli di aggiornamento dei Cms, dove il trend registrato per il 2021 appare essere in peggioramento rispetto al 2020. Se dunque, a livello macro la situazione che emerge pare essere caratterizzata da intrinseche fragilità tecniche, la fotografia scattata dall'Istat attraverso i dati ripresi dal censimento permanente sulle istituzioni pubbliche del 2020 (conclusosi ufficialmente il 15 settembre 2021, in materia di digitalizzazione, presenta dati aggiornati al 31 dicembre 2020), consente di sottolineare le differenze esistenti tra i diversi livelli di amministrazione (Fig. 1).

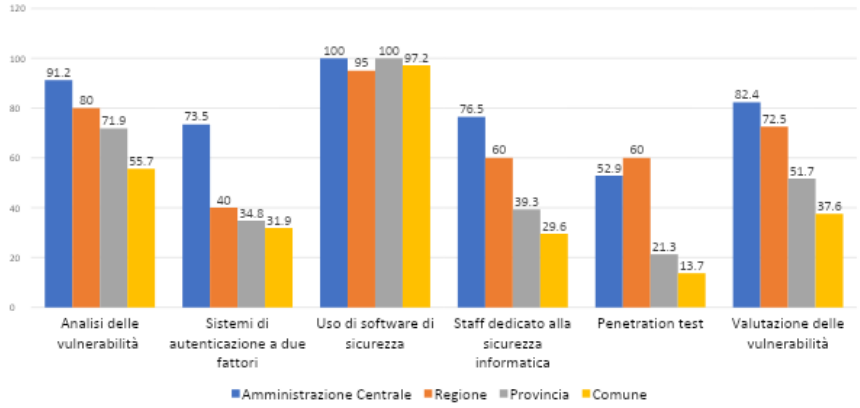

Fig. 1. Misure di sicurezza informatica di amministrazioni centrali e locali (distribuzioni percentuali). *Fonte*: Istat, Censimento permanente sulle istituzioni pubbliche, 2020.

Dai dati ciò che emerge sono le macroscopiche differenze nell'applicazione di misure di sicurezza informatica tra il livello centrale e i diversi livelli locali. La principale spiegazione nella disomogenea implementazione di azioni di prevenzione e contrasto alle minacce informatiche è da rinvenire nella diseguale disponibilità di risorse umane e materiali utilizzate dai diversi enti pubblici considerati. Nei fatti, si registrano significativi dislivelli tra amministrazioni centrali e locali sia sul fronte dell'analisi e valutazione delle vulnerabilità (si ha coscienza delle vulnerabilità informatiche nel 82,4% delle amministrazioni dello Stato a scapito di un ben più modesto 37,6% dei comuni) che nella presenza di staff qualificato (il 76,5% delle amministrazioni centrali possiede personale specializzato al fronte del 39,3% delle regioni e il 29,6% dei comuni). In questo modo salvo una generale diffusione di basici software di sicurezza (come gli antivirus), l'Istat registra il diffondersi di una embrionale cultura della sicurezza cibernetica solo nelle amministrazioni centrali dello Stato (le quali sono anche quelle più a rischio di attacco) e al più al livello regionale (affermatasi in risposta ai numerosi attacchi subiti alle infrastrutture predisposte alla gestione dell'emergenza sanitaria), lasciando la gran parte delle amministrazioni locali (soprattutto i comuni) in un contesto di arretratezza e vulnerabilità tecnologica. A livello generale e dall'analisi delle informazioni disponibili si scatta, dunque, la fotografia di un sistema amministrativo sotto assedio dal punto di vista digitale, in cui si paga ancora lo scotto di un certo ritardo nella diffusione di competenze e di un'adeguata cultura della sicurezza cyber, oltre ad una notevole differenziazione tra i diversi livelli amministrativi che lo compongono.

4. La strategia italiana di cybersicurezza

Se quanto riportato descrive la portata della minaccia e le principali criticità che rendono le amministrazioni pubbliche tecnicamente violabili, in questo paragrafo si proverà a definire quella che invece risulta essere la strategia perseguita dal policymaker italiano per impostare e migliorare i livelli di resilienza informatica del sistema paese. Nel contesto descritto dai dati, che si inserisce nel più ampio panorama di attivismo registrato sul piano comunitario, la sicurezza cibernetica costituisce, infatti, un fronte strategico e geopolitico di assoluta rilevanza, necessario ad accompagnare il processo di digitalizzazione del settore pubblico. In Italia, così come in ambito comunitario, gli anni che segnano un cambio di passo sul tema risultano essere quelli a partire dal 2013 (Cencetti 2014), i quali tuttavia sono preceduti da interventi anche molto precedenti, retrodatati tra gli inizi degli anni Novanta e gli anni Duemila, i quali testimoniano un lungo percorso di gestazione che solo di recente ha portato a una più strutturata policy sul tema (Renzi 2022).

Nei fatti i primi riferimenti normativi che introducono i concetti di minaccia cyber e di criminalità informatica, come nuove fattispecie giuridiche nell'ordinamento italiano, sono le Legge n. 547/1993 e Legge n. 268/1998. Esse, intervenendo sul Codice penale e sul Codice civile, determinano una maggiore attenzione alla diffusione dei reati attraverso gli strumenti informatici, attribuendo le principali competenze in materia di controllo e sicurezza sulla rete ad un organo ad hoc facente capo al Ministero dell'interno: la Polizia postale e delle telecomunicazioni. Ulteriori avanzamenti si registrano tra il 2002 e il 2003 quando l'attenzione del legislatore si sposta dai reati commessi tra privati a quelli diretti contro le informazioni custodite in formato digitale dalle amministrazioni pubbliche, introducendo una maggiore sensibilità al tema della tutela della privacy. È, infatti in quegli anni che vengono prodotti la Direttiva del presidente del Consiglio dei ministri del 16 gennaio 2002, emanata dal Dipartimento per l'innovazione e le tecnologie, il Codice sulla protezione dei dati personali (Dlgs n. 196/2003) e quello delle comunicazioni elettroniche (Dlgs n. 259/2003). Con tali provvedimenti si stabilisce per la prima volta che «le informazioni gestite dai sistemi informativi pubblici costituiscono una risorsa di valore strategico per il governo del paese» (Dpcm 16/01/2002), introducendo così un'esigenza politica di difesa delle infrastrutture informatiche e dei dati in possesso della PA. Sono state invitate, inoltre, tutte le amministrazioni a svolgere una prima autovalutazione dei propri livelli di sicurezza attivando le prime iniziative volte a diffondere standard minimi di garanzia, necessari a tutelare quelli che venivano definiti come interessi strategici del paese. Nel 2003 è stato, inoltre, istituito l'Osservatorio permanente per

la sicurezza e la tutela delle reti e delle comunicazioni che agiva sotto l'egida del Ministero dello sviluppo economico, con la partecipazione del Ministero della difesa e della Presidenza del consiglio. L'istituzione dell'Osservatorio, dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione, del Cert-Mise (ex art 16-bis del Codice delle comunicazioni elettroniche; nei fatti, poi, mai realizzato) e l'adozione della direttiva del 2002 richiamata, hanno fatto da apripista ai successivi interventi in materia (Cencetti 2014). Il tema venne, infatti, ripreso con la Legge n. 155/2005, la quale ha predisposto l'istituzione presso il Ministero dell'interno del Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (Cnaipic), operativo dal 2008. In questo modo si è evidenziato il nesso tra cybersecurity e protezione delle infrastrutture, tanto che nello stesso anno il Ministero dell'interno ha approvato un documento volto a stabilire le procedure per la classificazione delle infrastrutture informatiche di interesse nazionale. Un ulteriore e ben più deciso passo in avanti si è realizzato con l'approvazione del Codice dell'amministrazione digitale (Dlgs n. 82/2005) e la sua graduale realizzazione. Esso rappresentando un punto di riferimento normativo, oltre che un fondamentale catalizzatore per il processo di digitalizzazione del settore pubblico, non ha mancato di sottolineare l'importanza della sicurezza informatica (art. 51) al fine di assicurare una piena ed effettiva conversione in formato digitale dell'attività pubblica. Infatti, proprio il diffondersi sempre più massiccio delle tecnologie digitali, in combinato disposto con l'utilizzo e la raccolta dei dati nel settore pubblico, hanno ampliato i problemi connessi alla sicurezza, tanto da richiedere una radicale riorganizzazione della gestione degli interventi e della governance politica in materia. A testimonianza di ciò si richiama la relazione Copasir del 15 luglio del 2010 che, tra le raccomandazioni sul tema, suggerì l'adozione di «un impianto strategico-organizzativo che assicuri una leadership adeguata e predisponga chiare linee politiche per il contrasto alle minacce e il coordinamento tra gli attori interessati», comportando l'individuazione di una struttura di coordinamento, da istituire presso la Presidenza del Consiglio dei ministri che si occupasse di tutte le maggiori questioni di cybersecurity. Il Copasir segnalò, inoltre, anche i numerosi accordi di collaborazione e protocolli d'intesa, tra il settore pubblico e quello privato delineando tali iniziative come un aspetto caratterizzante l'approccio italiano, spesso non supportato dall'intervento legislativo (Cencetti 2014). Si può dunque dire che dall'analisi della prima fase si ricava una struttura di governance politico-amministrativa frammentata. Essa prevedeva diversi centri decisionali e una responsabilità politica spalmata su numerose strutture amministrative, tra cui le principali erano il Ministero dell'interno, il Ministero dello sviluppo economico e i dipartimenti interessati facenti capo alla Presidenza del Consiglio dei ministri (Funzione pubblica e

innovazione *in primis*). In più si registrava una linea d'intervento che lasciava ampio margine di manovra ai singoli enti e che mancava di una precisa struttura di coordinamento, condizionando i risultati ottenuti e creando situazioni di anche marcata differenza tra i diversi livelli amministrativi.

Se questo appare il quadro *ex ante*, a partire dal 2012-2013 si assiste ad un decisivo cambio di passo (Fig. 2). Una prima importante innovazione si realizza con l'istituzione, nel 2012, dell'Agenzia per l'Italia digitale (Agid) e alla predisposizione al proprio interno di un comparto definito Cert-PA (Computer emergency response team per la Pubblica amministrazione, divenuto operativo dal gennaio 2014), che aveva il compito di offrire una tempestiva risposta di trattamento per gli incidenti di sicurezza informatica che interessavano il dominio digitale delle Pubbliche amministrazioni. Si apriva in questo modo, anche su input comunitario (vedi par. 2), una stagione di intenso attivismo legislativo in materia, volto a realizzare una radicale riorganizzazione delle strutture interessate dalle policy di cybersicurezza, culminate con la definizione del perimetro di sicurezza nazionale cibernetica (Dl n. 105/2019) e l'Agenzia per la cybersicurezza nazionale (Dl n. 82/2021). Di seguito, al fine di organizzare al meglio le principali tappe di evoluzione sul tema, si è cercato di raccogliere in figura quelli che rappresentano i principali interventi politici e legislativi dal 2013 ad oggi.

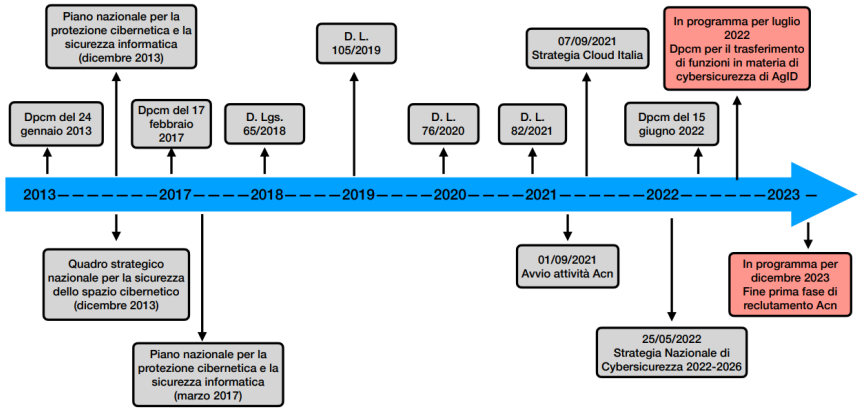

Fig. 2. Interventi legislativi e di policy in Italia in materia di cybersicurezza.
Fonte: elaborazione degli autori.

Il punto di partenza di questa rivoluzione copernicana si realizza con il Dpcm del 24 gennaio 2013 sulla «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale», in cui si predispone per la

prima volta una precisa architettura istituzionale deputata alla sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali. Tale architettura mette al vertice politico la Presidenza del Consiglio dei ministri seguita dal Comitato interministeriale per la sicurezza della repubblica (Cisr), oltre a predisporre una serie di organismi volti da un lato a prevenire i rischi attraverso la raccolta di informazioni e lo svolgimento di analisi: si pensi al Dipartimento delle informazioni per la sicurezza (Dis), all'Agenzia informazione sicurezza esterna (Aise) e all'Agenzia informazione sicurezza interna (Aisi); dall'altro a gestirne le risposte attraverso il Nucleo per la sicurezza cibernetica, il Nucleo interministeriale situazione e pianificazione (Nisp) e il Cert nazionale. In questo senso il disegno risalente all'allora governo Monti, sotto la spinta della Commissione europea, declinò la strategia italiana attraverso due documenti fondamentali: uno strategico, il «Quadro strategico nazionale per la sicurezza dello spazio cibernetico» ed uno operativo, il «Piano nazionale per la protezione cibernetica e la sicurezza informatica 2013», poi rivisto ed aggiornato nel 2017. Su queste fondamenta si inserisce l'ulteriore tassello della Direttiva Nis (*Network and information security* – Ue 2016/1148), recepita dall'Italia con il decreto legislativo n. 65/2018, a cui segue il richiamato intervento sull'istituzione del perimetro di sicurezza nazionale (Dl n. 105/2019). Esso è stato adottato attraverso due decreti del presidente del consiglio: il primo, il Dpcm del 30 luglio 2020, n. 131, ha definito i criteri e le modalità per l'individuazione dei soggetti inclusi nel perimetro; il secondo, il Dpcm del 14 aprile 2021, n. 81, ha predisposto le modalità per la notifica nel caso di incidenti riguardanti beni Tic. In questo modo si è cercato di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, oltre che degli enti e degli operatori nazionali, pubblici e privati, denotando una presa di coscienza politica della difesa nell'ambiente digitale come tutela strategica degli interessi nazionali. Ulteriore passo in avanti nell'istituzionalizzazione della governance della cybersecurity in Italia si realizza con la nascita dell'Agenzia per la cybersicurezza nazionale (Acn) attraverso il Dl n. 82/2021 (Parona 2021). Quest'ultimo intervento ha affinato la definizione dell'architettura nazionale di sicurezza digitale, razionalizzando la governance predisposta dal già richiamato Dpcm del 24 gennaio 2013, ripresa e approfondita nel successivo Dpcm del 17 febbraio 2017 (cd. Decreto Gentiloni), ed elevando significativamente gli standard di sicurezza al fine di raggiungere i target fissati a livello comunitario e internazionale. In questo senso la definizione dell'Acn ha risposto all'esigenza di raccordo politico e di coordinamento amministrativo tra i numerosi attori coinvolti, fornendo un'interfaccia unica a livello nazionale, europeo e internazionale in materia.

Essa, così come stabilito nella Strategia nazionale di cybersicurezza 2022-2026, si occupa di:

- assicurare il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza;
- promuovere, anche in un'ottica di rafforzamento della partnership pubblico-privato, la realizzazione di una cornice di sicurezza e resilienza cibernetiche per lo sviluppo della digitalizzazione del paese, del sistema produttivo e delle Pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica, a tutela degli interessi nazionali nel settore.

Le funzioni attribuite all'agenzia esprimono un approccio olistico alla gestione della cybersicurezza, nel quale acquistano rilevanza non solo gli interventi di natura prevalentemente tecnica, volti a garantire la sicurezza e la resilienza delle reti, dei sistemi informativi e dei servizi informatici, ma anche le progettualità finalizzate allo sviluppo di nuovi prodotti e tecnologie, della ricerca e della competitività industriale, nonché alla creazione di una forza lavoro nazionale di settore in grado di rispondere alle esigenze del mercato (Agenzia per la cybersicurezza nazionale 2022, 26-27). L'Acn diviene, inoltre, ancora più importante con la decisione di ampliare sempre più l'utilizzo della tecnologia cloud (Strategia cloud Italia del 9 settembre 2021) e la conseguente creazione di un Polo strategico nazionale per la sua gestione e salvaguardia, il quale prevede il coinvolgimento attivo dell'agenzia (Carotti 2022). Tutti questi interventi introducono una linea di demarcazione tra le attività di cyber-intelligence e quelle di cyber-resilience. Mentre le prime sono attribuite, a monte dalla Legge n. 124/2007, successivamente modificata dalla Legge n. 133/2012, agli organismi di informazione e sicurezza, mentre le seconde sono state affidate al nuovo soggetto, verso il quale sono confluiti il Nucleo per la cybersicurezza, quale luogo di coordinamento e gestione delle crisi cibernetiche nazionali, e il Csirt-Italia (Presidenza del Consiglio dei ministri 2022, 43). Con la realizzazione dell'Acn si porta, dunque, a compimento un disegno istituzionale in materia di cybersicurezza più coerente ed efficiente, necessario a rafforzare le capacità di difesa nazionale, rinvigorendo il coordinamento politico e tecnico tra i soggetti coinvolti. Per tale ragione l'Acn, che ha iniziato a muovere i suoi primi passi solo dalla fine del 2021 (l'ente è entrato in funzione il 1° settembre 2021, con le prime nomine arrivate tra la fine del 2021 e l'inizio del 2022), ha seguito una marcia a tappe forzate. Il ritmo incalzante dei cambiamenti ha portato alla pubblicazione, il 25 maggio 2022, della già richiamata Strategia nazionale di cybersicurezza 2022-2026, all'emanazione il 15 giugno 2022 del Dpcm per il trasferimento di funzioni operative dal Mise e, il 30 giu-

gno 2022, all'attivazione del Centro di valutazione e certificazione nazionale per la valutazione di beni, sistemi e servizi Ict destinati alle funzioni essenziali dello Stato. Ulteriori sforzi di implementazione dei poteri e della struttura amministrativa dell'agenzia sono previsti entro la fine del 2023 con l'emanazione del Dpcm per il trasferimento delle competenze in materia di cybersicurezza dall'Agid (entro luglio 2022) e la chiusura della prima fase di reclutamento del personale (entro dicembre 2023). Tali passaggi testimoniano l'importanza nevralgica ritagliata a questa struttura. Ad essa, infatti, si delegano funzioni di rilevanza strategica e geopolitica fondamentali in virtù dei rapidi cambiamenti tecnologici che interessano, e sempre più interesseranno, il settore pubblico (si pensi agli ambiziosi target posti all'interno del Piano triennale per l'informatica nella PA 2021-2023) e all'enorme quantità di risorse che il paese è chiamato a gestire nella realizzazione del Pnrr, da utilizzare tassativamente entro il 2026.

5. Conclusioni

Giunti a conclusione di questo percorso, è possibile affermare che l'avanzamento tecnologico, grazie alla sua pervasività, determina profondi cambiamenti sociali, politici ed economici. Contestualmente, la portata di tali mutamenti comporta l'emersione di rischi accentuati in relazione alla sicurezza complessiva del settore pubblico. Nei fatti, circoscrivere la portata del fenomeno e padroneggiarne le implicazioni gioca un ruolo cruciale nella definizione di strategie di intervento efficaci e ad impatto diretto sulla definizione degli equilibri geopolitici mondiali. Nell'ambito di questo contesto, l'Ue sta tentando di assumere una posizione di coordinamento delle policy nazionali, con l'obiettivo di definire quella che in futuro ambisce a divenire un'autonoma politica di sicurezza comune a livello europeo. Il tema appare ancora in itinere poiché, data la sua rilevanza per l'affermazione della sovranità statale, le ambizioni europee si scontrano con i limiti politici del suo progetto. Non si può non sottolineare come per l'Ue il tema della sicurezza e della politica di difesa risulti accompagnato ancora da una gelosa tutela delle prerogative nazionali degli Stati membri, oltre ad aver accumulato un notevole ritardo (da recuperare) rispetto agli altri giganti mondiali (come la Cina o la Russia), dovuto ad una sostanziale subordinazione di percorso nei confronti dello storico alleato statunitense.

In questo ambito, il digitale ha impattato stravolgendo i vecchi rapporti di forza, ponendo i singoli Stati europei dinanzi a sfide che da soli non sono in grado di fronteggiare. Nello specifico, l'Italia ne rappresenta un caso emblematico. Essa, infatti, pur scontando un'eredità di cronico ritardo digitale nel

settore pubblico, ha intrapreso negli ultimi anni un percorso di importante accelerazione, prendendo coscienza della definizione di una politica di sicurezza anche in ambito cibernetico. Nonostante siano stati compiuti numerosi passi in avanti nell'istituzionalizzazione di una ben più strutturata policy di cybersicurezza, attraverso l'individuazione di chiare responsabilità politiche e la creazione di nuovi attori, quest'impegno si scontra con la realtà empirica emergente dai dati. Ciò evidenzia un sistema ancora molto fragile sotto il profilo informatico, nel quale però si segnalano dei primi timidi, eppure importanti, investimenti volti a colmare tale gap, che tuttavia da soli non potranno bastare a resistere in un ambiente dominato da grandi potenze internazionali.

Per concludere, l'ambiente digitale assume dunque le sembianze di un grande campo di battaglia, in cui le amministrazioni pubbliche dei singoli Stati appaiono essere «sotto assedio digitale», subendo livelli di ingerenza mai sperimentati prima nella storia. Nessun problema è emerso tanto rapidamente nella sua importanza come quello della cybersicurezza. Tuttavia, ancora oggi, non esiste alcuna problematica così poco compresa come quella relativa alla sicurezza informatica (Singer e Friedman 2014).

Riferimenti bibliografici

Agenzia per la cybersicurezza nazionale (2022), *Piano di Implementazione Strategia Nazionale di Cybersicurezza 2022-2026*, https://www.acn.gov.it/ACN_Strategia.pdf. Consultato il 5 agosto 2022.

Bozzetti, M. R., Olivieri, L. e Spoto, F. (2021), *Cybersecurity Impacts of the Covid-19 Pandemic in Italy*, paper presentato alla V Conferenza italiana sulla cybersicurezza (Itasec), Online, 7-9 aprile.

Calise, M. (2021), *Virus contro virus*, in «Rivista di Digital Politics», 1(1), pp. 5-20.

Calise, M. e Musella, F. (2019), *Il principe digitale*, Roma-Bari, Laterza.

Carotti, B. (2020), *Sicurezza cibernetica e Stato nazione*, in «Giornale di Diritto Amministrativo», pp. 629-641.

Carotti, B. (2022), *Il settore pubblico e il cloud computing*, in V. Bontempi (a cura di), Lo Stato Digitale nel Piano Nazionale di Ripresa e Resilienza, Roma, Roma Tre Press, pp. 147-155.

Cencetti, C. (2014), *Cybersecurity: Unione europea e Italia: Prospettive a confronto (Vol. 12)*, Roma, Edizioni Nuova Cultura.

Cert-Agid (2021), *Secondo Monitoraggio dello Stato di Aggiornamento del Protocollo Https e dei Cms sui Sistemi della PA*, https://cert-agid.gov.it/news/secondo-monitoraggio-dello-stato-di-aggiornamento-del-protocollo-https-e-dei-cms-sui-sistemi-della-pa. Consultato il 5 agosto 2022.

Craigen, D., Diakun-Thibault, N. e Purse, R. (2014), *Defining cybersecurity*, in «Technology Innovation Management Review», 4(10), pp. 13-21.

De Masi, D. (2020), *Smart working: La rivoluzione del lavoro intelligente*, Venezia, Marsilio.

Di Mascio, F., Angeletti, S. e Natalini, A. (2021), *Lo smart working nelle pubbliche amministrazioni centrali ai tempi del Covid-19*, in «Rivista Italiana di Politiche Pubbliche», 16(1), pp. 95-125.

European court of auditors (2019), *Challenges to effective Eu cybersecurity policy*, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf. Consultato il 5 agosto 2022.

European cyber security organisation (2020a), *Ecso Barometer 2020: «Cybersecurity in Light of Covid-19»: Report on the results of surveys with Ecso members and the cybersecurity community*. https://www.ecs-org.eu/documents/uploads/report-on-the-ecso-members-and-the-community-survey.pdf. Consultato il 5 agosto 2022.

European cyber security organisation (2020b), *Input to the Digital Europe Programme 2021-2027: Priorities for supporting the implementation of policy, technology, competitiveness, and competence-building*. Working Group 6 – Sria and Cybersecurity Technologies, https://ecs-org.eu/documents/publications/5fdc4ca16dde0.pdf. Consultato il 5 agosto 2022.

European union agency for cybersecurity (2022), *Research and Innovation Brief: Annual Report on Cybersecurity Research and Innovation Needs and Priorities*, https://www.enisa.europa.eu/publications/research-and-innovation-brief. Consultato il 5 agosto 2022.

Istat (2021), *Censimento permanente delle istituzioni pubbliche: risultati preliminari 2020*, l'anno dello smart working, https://www.istat.it/it/archivio/264696. Consultato il 5 agosto 2022.

Kasper, A. (2020), *Eu cybersecurity governance-stakeholders and normative intentions towards integration*, in M. Harwood, S. Moncada e R. Pace, (a cura di), *The future of the European Union: Demisting the Debate*, Msida, Institute for European Studies, pp. 166-185.

Kemmerer, R. A. (2003), *Cybersecurity, paper presentato alla 25th International conference on software engineering* (Icse 03), Portland, Oregon, 3-10 maggio.

Lanza, C. e Daille, B. (2019), *Terminology systematization for Cybersecurity domain in Italian language*, paper presentato alla Conférence sur le Traitement Automatique des Langues Naturelles (Taln-Recital), Toulouse, Francia, 1-5 luglio.

Markopoulou, D., Papakonstantinou, V. e De Hert, P. (2019), *The new EU cybersecurity framework: The NIS Directive, Enisa's role and the General Data Protection Regulation*, in «Computer Law & Security Review», 35, pp. 1-11.

Parona, L. (2021), *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, in «Giornale di Diritto Amministrativo», 6, pp. 709-720.

Peslak, A. e Hunsinger, D. S. (2019), *What Is Cybersecurity and What Cybersecurity Skills Are Employers Seeking?*, in «Issues in Information Systems», 20(2), pp. 62-72.

Presidenza del Consiglio dei ministri (2022), *Relazione Annuale sulla Politica dell'Informazione per la Sicurezza 2021*, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2022/02/RELAZIONE-ANNUALE-2021.pdf. Consultato il 5 agosto 2022.

Ramadan, R. A., Aboshosha, B. W., Sulaiman Alshdukhi, J., Alzahrani, A. J., El-Sayed, A. e Dessouky, M. M. (2021), *Cybersecurity and Countermeasures at the Time of Pandemic*, in «Journal of Advanced Transportation», pp. 1-19.

Renzi, A. (2021a), *Le prospettive europee sugli usi militari dell'intelligenza artificiale*, Osservatorio sullo Stato Digitale, Istituto di Ricerche sulla Pubblica amministrazione, 4 febbraio, https://www.irpa.eu/le-prospettive-europee-sugli-usi-militari-dellintelligenza-artificiale. Consultato il 5 agosto 2022.

Renzi, A. (2021b), *Slaughterbots e il futuro della guerra automatizzata*, Osservatorio sullo Stato Digitale, Istituto di Ricerche sulla Pubblica amministrazione, 26 gennaio 2021, https://www.irpa.eu/slaughterbots-e-il-futuro-della-guerra-automatizzata. Consultato il 5 agosto 2022.

Renzi, A. (2021c), *La sicurezza cibernetica: lo stato dell'arte*, in «Giornale di Diritto Amministrativo», 4/2021, pp. 538-548.

Renzi, A. (2022), *Le prospettive della cybersecurity*, in V. Bontempi (a cura di), *Lo Stato Digitale nel Piano Nazionale di Ripresa e Resilienza*, Roma, Roma Tre Press, pp. 157-169.

Schatz, D., Bashroush, R. e Wall, J. (2017), *Towards a more representative definition of cyber security*, in «Journal of Digital Forensics, Security and Law», 12(2), 8, pp. 53-74.

Schlehahn, E. (2020), *Cybersecurity and the State*, in M. Christen, B. Gordijn e M. Loi (a cura di), *The Ethics of Cybersecurity*, Cham, Springer, pp. 205-225.

Sgueo, G. (2022), *I servizi pubblici digitali*, in V. Bontempi (a cura di), *Lo Stato Digitale nel Piano Nazionale di Ripresa e Resilienza*, Roma, Roma Tre Press, pp. 119-125.

Singer, P. W. e Friedman, A. (2014), , Oxford, Oxford University Press.

Spafford, E. H. e Dewdney, A. K. (1989), *Computer recreations: of worms, viruses and core war*, in «Scientific American», 260(3), pp. 110-113.

Williams, T. D. (2020), *Epistemological Questions for Cybersecurity*, paper presentato alla 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Dublino, Irlanda, 15-19 giugno.